

25.11.2004

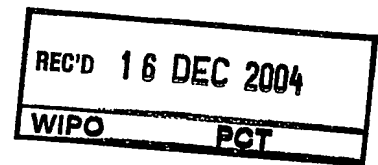
日 本 国 特 許 庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

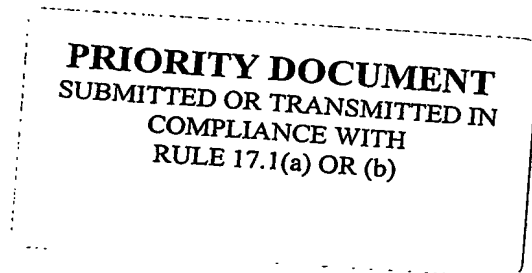
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日  
Date of Application: 2 0 0 3 年 1 1 月 2 0 日

出 願 番 号  
Application Number: 特 願 2 0 0 3 - 3 9 0 2 1 6  
[ST. 10/C]: [J P 2 0 0 3 - 3 9 0 2 1 6]



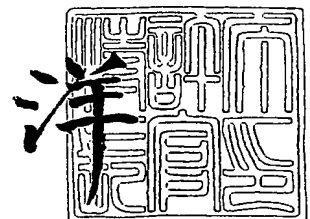
出 願 人  
Applicant(s): 日 本 電 気 株 式 有 限 公 司



2 0 0 4 年 9 月 2 9 日

特許庁長官  
Commissioner,  
Japan Patent Office

小 川



BEST AVAILABLE COPY

【書類名】 特許願  
【整理番号】 33510019  
【あて先】 特許庁長官殿  
【国際特許分類】 H04M 3/00  
H04L 9/00

【発明者】  
【住所又は居所】 東京都港区芝五丁目 7 番 1 号 日本電気株式会社内  
【氏名】 須田 幸憲

【発明者】  
【住所又は居所】 東京都港区芝五丁目 7 番 1 号 日本電気株式会社内  
【氏名】 百名 盛久

【特許出願人】  
【識別番号】 000004237  
【氏名又は名称】 日本電気株式会社

【代理人】  
【識別番号】 100093595  
【弁理士】  
【氏名又は名称】 松本 正夫

【手数料の表示】  
【予納台帳番号】 057794  
【納付金額】 21,000円

【提出物件の目録】  
【物件名】 特許請求の範囲 1  
【物件名】 明細書 1  
【物件名】 図面 1  
【物件名】 要約書 1  
【包括委任状番号】 9303563

**【書類名】 特許請求の範囲****【請求項 1】**

無線基地制御局と、前記無線基地制御局に接続される無線基地局とから構成され、前記無線基地局と接続可能な移動端末に対して移動通信サービスを提供する移動通信システムにおいて、

前記無線基地局を私設網内に配置し、前記私設網に設置された中継ノードにより前記私設網上を伝送される前記無線基地制御局と前記無線基地局間の移動通信トラフィックの中継を行い、前記移動端末が発呼あるいは着呼した際に、前記中継ノードが前記私設網内の帯域管理機能と連携した受け付け判定処理を行い、受付が許可された場合に前記移動端末に通信回線を提供することを特徴とする移動通信システム。

**【請求項 2】**

前記移動端末が発呼あるいは着呼した際に、前記無線基地制御局が前記無線基地局宛に送信した帯域制御シグナリングを前記中継ノードが受信することで、前記受付判定処理を起動することを特徴とする請求項 1 に記載の移動通信システム。

**【請求項 3】**

前記中継ノードが、VPNゲートウェイであることを特徴とする請求項 1 又は請求項 2 に記載の移動通信システム。

**【請求項 4】**

無線基地制御局と、前記無線基地制御局に接続される無線基地局とから構成され、前記無線基地局と接続可能な移動端末に対して移動通信サービスを提供する移動通信システムにおいて、

前記無線基地局を私設網内に配置し、前記私設網に設置された中継ノードにより前記私設網上を伝送される前記無線基地制御局と前記無線基地局間の移動通信トラフィックの中継を行い、

前記無線基地制御局と前記中継ノード間では第 1 の暗号鍵を、前記無線基地局と中継ノード間では第 2 の暗号鍵を用いて暗号化通信を行い、

前記第 2 の暗号鍵の生成に必要な秘匿鍵を前記無線基地制御局と前記無線基地局間の鍵交換メカニズムにより生成し、前記無線基地制御局が前記中継ノードに前記秘匿鍵を通知することを特徴とする移動通信システム。

**【請求項 5】**

無線基地制御局と、前記無線基地制御局に接続される無線基地局とから構成され、前記無線基地局と接続可能な移動端末に対して移動通信サービスを提供する移動通信システムにおいて、

前記無線基地局を私設網内に配置し、前記無線基地局と前記私設網を介して接続される中継ノードと前記無線基地局間の前記移動通信トラフィックは前記私設網内を伝送され、前記中継ノードにより前記私設網上を伝送される前記無線基地制御局と前記無線基地局間の移動通信トラフィックの中継を行い、

前記無線基地制御局と前記中継ノード間では第 1 の暗号鍵を、前記無線基地局と中継ノード間では第 2 の暗号鍵を用いて暗号化通信を行い、

前記第 2 の暗号鍵を前記無線基地制御局と前記無線基地局間の鍵交換メカニズムにより動的に生成し、前記無線基地制御局が前記中継ノードに前記第 2 の暗号鍵を通知することを特徴とする移動通信システム。

**【請求項 6】**

前記無線基地制御局が、

前記暗号鍵の生成に必要な事前共有鍵を前記無線基地局との間で鍵交換メカニズムを用いて動的に生成する手段と、前記事前共有鍵を前記中継ノードに通知する手段とを備えることを特徴とする請求項 4 又は請求項 5 に記載の移動通信システム。

**【請求項 7】**

前記無線基地制御局が、

前記無線基地局との間で鍵交換メカニズムを用いて動的に前記暗号鍵を生成する手段と

、前記暗号鍵を前記中継ノードに通知する手段とを備えることを特徴とする請求項4又は請求項5に記載の移動通信システム。

【請求項8】

無線基地局と無線基地制御局間の移動通信トラヒックの中継を行う中継ノードにおいて

、前記無線基地局が設置される私設網に設置され、前記私設網上を伝送される前記無線基地制御局と前記無線基地局間の移動通信トラヒックの中継を行い、

前記無線基地制御局が前記無線基地局宛に送信した帯域制御シグナリングを受信する手段と、

該帯域制御シグナリングに含まれるトラヒック情報を抽出する手段と、

私設網内の帯域管理機構と連携して受け付け判定を行う手段と、

前記受付判定結果と前記受付許可された帯域制御情報を含む帯域制御シグナリングを送信する手段とを備えることを特徴とする中継ノード。

【請求項9】

無線基地局と無線基地制御局間の移動通信トラヒックの中継を行う中継ノードにおいて

、前記無線基地局が設置される私設網に設置され、前記私設網上を伝送される前記無線基地制御局と前記無線基地局間の移動通信トラヒックの中継を行い、

無線基地局と無線基地制御局に接続され、前記無線基地局とは第1の暗号鍵を、前記無線基地制御局とは第2の暗号鍵を用いて暗号化通信を行い、

前記無線基地制御局から前記第1の暗号鍵を生成するための事前共有鍵を受け取る手段と、前記事前共有鍵を用いて前記無線基地局との間で前記第1の暗号鍵を動的に生成する手段と、前記第1の暗号鍵を用いて前記移動通信トラヒックの暗号化を行う手段とを備えることを特徴とする中継ノード。

【請求項10】

無線基地局と無線基地制御局間の移動通信トラヒックの中継を行う中継ノードにおいて

、前記無線基地局が設置される私設網に設置され、前記私設網上を伝送される前記無線基地制御局と前記無線基地局間の移動通信トラヒックの中継を行い、

無線基地局と無線基地制御局に接続され、前記無線基地局とは第1の暗号鍵を、前記無線基地制御局とは第2の暗号鍵を用いて暗号化通信を行い、

前記第1の暗号鍵を前記無線基地制御局から受け取る手段と、前記第1の暗号鍵を用いて前記移動通信トラヒックの暗号化を行う手段とを備えることを特徴とする中継ノード。

【請求項11】

複数の無線基地局と異なる暗号鍵を用いて暗号化通信を行う中継ノードを介して、前記無線基地局と接続される無線基地制御局において、

前記暗号鍵の生成に必要となる事前共有鍵を前記無線基地局との間で鍵交換メカニズムを用いて動的に生成する手段と、前記事前共有鍵を前記中継ノードに通知する手段とを備えることを特徴とする無線基地制御局。

【請求項12】

複数の無線基地局と異なる暗号鍵を用いて暗号化通信を行う中継ノードを介して、前記無線基地局と接続される無線基地制御局において、

前記無線基地局との間で鍵交換メカニズムを用いて動的に前記暗号鍵を生成する手段と、前記暗号鍵を前記中継ノードに通知する手段とを備えることを特徴とする無線基地制御局。

【請求項13】

無線基地局と無線基地制御局間の移動通信トラヒックの中継を行う中継ノードで実行される中継ノード用プログラムであって、

無線基地局が設置される私設網に設置され、前記私設網上を伝送される無線基地制御局と前記無線基地局間の移動通信トラヒックの中継を行う機能と共に、

前記無線基地制御局が前記無線基地局宛に送信した帯域制御シグナリングを受信する機能と、前記帯域制御シグナリングに含まれるトラフィック情報を抽出する機能と、私設網内の帯域管理機構と連携して受け付け判定を行う機能と、前記受付判定結果と前記受付許可された帯域制御情報を含む帯域制御シグナリングを送信する機能とを有することを特徴とする中継ノード用プログラム。

【請求項 14】

無線基地局と無線基地制御局間の移動通信トラフィックの中継を行う中継ノードで実行される中継ノード用プログラムであって、

無線基地局が設置される私設網に設置され、前記私設網上を伝送される無線基地制御局と前記無線基地局間の移動通信トラフィックの中継を行い、前記無線基地局とは第1の暗号鍵を、前記無線基地制御局とは第2の暗号鍵を用いて暗号化通信を行う機能と共に、

前記無線基地制御局から前記第1の暗号鍵を生成するための事前共有鍵を受け取る機能と、前記事前共有鍵を用いて前記無線基地局との間で前記第1の暗号鍵を動的に生成する機能と、前記第1の暗号鍵を用いて前記移動通信トラフィックの暗号化を行う機能とを有することを特徴とする中継ノード用プログラム。

【請求項 15】

無線基地局と無線基地制御局間の移動通信トラフィックの中継を行う中継ノードで実行される中継ノード用プログラムであって、

無線基地局が設置される私設網に設置され、前記私設網上を伝送される無線基地制御局と前記無線基地局間の移動通信トラフィックの中継を行い、前記無線基地局とは第1の暗号鍵を、前記無線基地制御局とは第2の暗号鍵を用いて暗号化通信を行う機能と共に、

前記第1の暗号鍵を前記無線基地制御局から受け取る機能と、前記第1の暗号鍵を用いて前記移動通信トラフィックを暗号化する機能とを有することを特徴とする中継ノード用プログラム。

【請求項 16】

複数の無線基地局と異なる暗号鍵を用いて暗号化通信を行う中継ノードを介して、前記複数の無線基地局と接続される無線基地制御局で実行されるプログラムであって、

前記暗号鍵の生成するために必要な事前共有鍵を前記無線基地局との間で鍵交換メカニズムを用いて動的に生成する機能と、前記事前共有鍵を前記中継ノードに通知する機能とを有することを特徴とする無線基地制御局用プログラム。

【請求項 17】

複数の無線基地局と異なる暗号鍵を用いて暗号化通信を行う中継ノードを介して、前記複数の無線基地局と接続される無線基地制御局に使用されるプログラムであって、

前記無線基地局との間で鍵交換メカニズムを用いて動的に前記暗号鍵を生成する機能と、前記暗号鍵を前記中継ノードに通知する機能とを有することを特徴とする無線基地制御局用プログラム。

**【書類名】明細書**

**【発明の名称】** 移動通信システム、中継ノード、無線基地制御局、中継ノード用プログラム、無線基地制御局用プログラム

**【技術分野】****【0001】**

本発明は、複数の無線基地制御局と、1つの無線基地制御局に接続される複数の無線基地局とから構成され、無線基地局と接続可能な移動端末に対して移動通信サービスを提供する移動通信システムに関し、特に、私設網を利用して屋内エリア内のユーザに対して移動通信サービスを提供することを可能にする移動通信システムに関する。

**【背景技術】****【0002】**

移動通信システムでは、ビル等の屋内の内部まで電波が届きにくいいため、屋内で移動端末を使用するユーザは安定した移動通信サービスを受けることができない。屋内のユーザに対して安定した移動通信サービスを提供するためには、屋内をカバーするための移動通信専用の屋内システムの導入が必要となる。特に、2GHz帯を使用する3Gサービスは2Gサービスと比べて、電波伝搬特性が良くないため、不感地帯となる屋内エリアが多くなる。

**【0003】**

このような状況において、3Gサービスの屋内エリアを2Gサービスと同等にするためには、屋内システムを多数導入することが必要となるが、それに応じて移動通信オペレータを多数配置することはコスト的な点で実現が難しい。そのため、より低コストな屋内システムが要求されている。

**【0004】**

UMTSの標準化を行っている3GPPでは、無線基地制御局(RNC)と無線基地局間をIP網で接続可能とするIPトランスポートオプションを提供するリリース5が定義された。そこで、IPトランスポートを利用した屋内システムの1つのアプローチとして、屋外回線に公衆インターネット網や閉域IP網、屋内回線にLAN等の私設網(例えば、企業等が自身で私的に構築したネットワーク等)を利用する形態が考えられる。これにより、回線敷設コストを大幅に削減でき、屋内システムの導入コストを大幅に低減可能となる。

**【0005】**

このような私設網(ネットワーク)を用いた移動通信システムでは、以下に示す新たな機能が要求される。

- (1) 私設網における移動通信トラヒックの帯域制御
- (2) 私設網内のファイアウォール/NAPT(Network Address Port Translation)を越えた無線基地制御局—無線基地局間通信の実現
- (3) 移動通信トラヒックのセキュリティ確保
- (4) 移動通信オペレータが移動通信ノードに対して独自に割り当てたIPアドレス体系の維持

**【0006】**

上記(1)の機能に関して、私設網での帯域制御方法として、ポリシーサーバによる集中型帯域制御方式が一般的である。本方式は、ポリシーサーバがルータやイーサネット(R)スイッチ等のLANデバイスに対してパケット識別に必要なトラヒック情報と帯域制御ルールを含む帯域制御情報を事前に配布し、私設網のエッジに位置するLANデバイスがトラヒック情報に基づきエンドホストあるいはインターネットから受信したパケットのIPヘッダとL4ヘッダを用いてパケット識別を行い、該当する帯域制御情報に応じたマークをパケットに付加した後、次ホップのLANデバイスに転送する。エッジでないLANデバイスは、エッジのLANデバイスが付加したマークとポリシーサーバから配布された帯域制御情報に基づきパケット単位で帯域制御を行うものである。

**【0007】**

上記(2)～(4)の機能に関しては、例えばIPsecベースのVPN(Virtual Private Network: 仮想私設ネットワーク)技術を利用することで実現可能である。具体的には、VPNゲートウェイを私設網の管轄外に設置し、無線基地制御局と無線基地局は常にVPNゲートウェイを介して通信を行い、無線基地制御局とVPNゲートウェイ間、無線基地制御局と無線基地局間においてIPsecによる暗号化通信技術を適用することで実現できる。

【0008】

なお、従来の移動通信システムの例としては、例えば、セキュリティを維持しつつ、無線端末装置と有線端末装置間で通信を行うための技術が、特開2001-333110号公報(特許文献1)等の開示されている。

【0009】

従来の移動データ通信における仮想私設網の構成方法に関する技術が、例えば特開平10-032610号公報(特許文献2)の開示されている。

【特許文献1】特開2001-333110号公報

【特許文献2】特開平10-032610号公報

【発明の開示】

【発明が解決しようとする課題】

【0010】

上記の帯域制御方式において、移動通信トラフィックが私設網の帯域の大半を占有した場合、私設網の回線が輻輳し、無線基地制御局－無線基地局間の移動通信トラフィックの通信品質が劣化する、あるいは他の私設網内のトラフィックに支障をきたす可能性がある。

【0011】

また、上記のVPN方式では、無線基地制御局及び無線基地局が複数存在する場合、無線基地制御局と無線基地局間の経路制御情報をVPNゲートウェイに、第三者認証を利用せずに無線基地制御局－VPNゲートウェイ間とVPNゲートウェイ－無線基地局間でのIPsec SA(Security Association)を確立する上で必要となる事前共有鍵をVPNゲートウェイに予め設定しておく必要があり、設置する無線基地局の台数が多くなった場合に、屋内システムの導入時の作業が煩雑になる。

【0012】

本発明の目的は、私設網を用いて移動通信サービスを提供するに当たり、移動通信トラフィックの増大に起因して私設網内回線が輻輳するのを防ぎ、他のトラフィックにも支障をきたさない移動通信システムを提供することにある。

【0013】

本発明の他の目的は、設置する無線基地局の台数が多くなった場合にも、屋内システムの導入時の作業を簡易化することができる移動通信システムを提供することにある。

【課題を解決するための手段】

【0014】

本発明によれば、移動端末が発呼/着呼した際に、無線基地制御局と無線基地局間の移動通信制御シグナリングを中継ノードであるVPNゲートウェイが終端し、シグナリングに含まれるトラフィック情報をポリシーサーバに通知すると共に、受付判定を要求する。ポリシーサーバが受付を許可した場合のみ、移動端末に通信回線を提供することにより、上記の目的を達成する。

【0015】

本発明の他の態様によれば、中継ノードであるVPNゲートウェイと無線基地制御局間に既にSAが確立されている状態で、無線基地局を起動すると、VPNゲートウェイに対して転送先無線基地制御局を指定した後、SA確立処理を開始し、VPNゲートウェイは、SAを確立するためのIKE(Internet Key Exchange)シグナリングを、指定された転送先無線基地制御局に転送し、無線基地制御局が代理でSAを確立し、VPNゲートウェイに対して確立したSA情報を通知する。

【0016】

あるいは、無線基地局と無線基地制御局間でSAの確立に必要な事前共有鍵を動的に生成し、無線基地制御局がVPNゲートウェイに事前共有鍵を通知し、VPNゲートウェイはこれを用いて無線基地局との間でSAを動的に確立する。このように、VPNゲートウェイは無線基地制御局より通知されたSA情報、あるいは配布された事前共有鍵を用いて確立したSA情報に基づき、無線基地局との間で暗号化通信を行うことにより、上記の目的を達成する。

#### 【発明の効果】

##### 【0017】

本発明の第1の効果は、無線基地局と無線基地制御局間の回線として私設網を用いて移動通信サービスを提供するに当たり、移動通信トラヒックに起因して私設網内の回線が輻輳するのを防ぎ、他のトラヒックに支障をきたさないことである。これは、移動端末が発呼／着呼した際に、無線基地制御局が送信する移動通信制御シグナリングを中継ノードであるVPNゲートウェイが受信し、移動端末の通信に必要な帯域をポリシーサーバに通知すると共に、受付判定を要求し、受付判定の結果に応じて移動端末の通信回線を提供するか否かを決定するためである。

##### 【0018】

本発明の第2の効果は、屋内システムの導入時の作業を簡易化できることである。これは、無線基地局が起動すると、中継ノードであるVPNゲートウェイに対してIKEシグナリングを転送する依頼した後、無線基地局とVPNゲートウェイ間で利用するSAを無線基地局と無線基地制御局間で確立し、無線基地制御局が確立したSA情報をVPNゲートウェイに通知すると共に、VPNゲートウェイは通知されたSA情報を利用して無線基地局と暗号化通信を行うようにしたためである。あるいは、IPsec SA確立に必要な事前共有鍵を無線基地局と無線基地制御局間で鍵交換メカニズムにより動的に生成し、無線基地制御局が生成した事前共有鍵をVPNゲートウェイに通知し、VPNゲートウェイは配布された事前共有鍵を用いて無線基地局との間にIPsec SAを確立し、暗号化通信を行うためである。

#### 【実施例】

##### 【0019】

図1及び2に示すネットワーク構成図を用いて本発明の第1の実施例に係わる移動通信システムを説明する。PC110等が接続された私設の網であるLAN20は、イーサネット(R) (Ethernet(R)) で構築されており、ファイアウォール90、VPN(Virtual Private Network)ゲートウェイ(GateWay)100を介してインターネット網10と接続されている。一方、移動通信コア網30は無線基地制御局(無線基地制御局:Radio Network Controllerと称する)70と移動網ゲートウェイ120を介してインターネット網10と接続されている。

##### 【0020】

また、無線基地局60～63は私設網(私設ネットワーク、例えば企業が私的に構築したネットワーク)としてのLAN20に接続され、無線基地制御局70と無線基地局60～63間の通信では、インターネット網10及びLAN20を回線として利用し、VPNゲートウェイ100を介することでファイアウォール90を越えた通信を行う。このような形態で、移動通信オペレータは移動端末80に対してインターネットアクセス等のデータ通信サービスを提供する。

##### 【0021】

さらに、LAN20内はプライベートアドレスで運用されており、インターネット網10はグローバルアドレスで運用されている。無線基地制御局70と無線基地局60～63間の通信では、セキュリティを確保するためIPsec ESP(Encapsulation Security Payload)トンネルモードを利用し、インターネット網10では外部IPヘッダにグローバルIPアドレスを、LAN20ではプライベートIPアドレスを使用し、内部IPヘッダにはオペレータが無線基地制御局70及び無線基地局60～63に独自に割り当てたIPアドレス(以降、オペレータ独自アドレスと称する)を使用する。



**【0022】**

L A N 2 0 は例えば図 2 のように構成される。図示するように、L A N 2 0 はルータ 2 1 0 と複数の E t h e r n e t (R) スイッチ 2 2 0 ~ 2 2 3 で構成されており、無線基地局 6 0 と P C 1 1 0 はそれぞれ E t h e r n e t (R) スイッチ 2 2 1、2 2 3 に接続されている。(記述を簡略化するため、以降ではルータ 2 1 0 と E t h e r n e t (R) スイッチ 2 2 0 ~ 2 2 3 を総称して L A N デバイスと呼ぶ。) また、L A N 2 0 では帯域制御が行われており、本実施例ではポリシーサーバ 2 0 0 による集中型の帯域制御を行っている場合を示している。その場合、ポリシーサーバ 2 0 0 にはトラヒックの特性が記述されたトラヒック情報とそのトラヒックに対して帯域制御を行う上で必要となる帯域制御情報が予め設定されており、ポリシーサーバ 2 0 0 は L A N デバイスの起動を検出すると、C O P S (Common Open Policy Service) プロトコルを用いてトラヒック情報と帯域制御情報を L A N デバイスに配信し、各 L A N デバイスは通知された帯域制御情報に基づいて受信したパケットに対して帯域制御を行う。

**【0023】**

また、各 L A N デバイスは帯域の制御状態を S N M P (Simple Network Management Protocol) によりポリシーサーバ 2 0 0 にレポートし、ポリシーサーバ 2 0 0 は L A N 2 0 全体の帯域制御状態を集中的に管理する。L A N 2 0 を流れる移動通信トラヒックに対しても同様の帯域制御が行われる。移動通信トラヒックにはシグナリングデータとユーザデータの 2 種類がある。シグナリングデータトラヒックに関しては以下に述べる手法により帯域制御を行う。予めポリシーサーバ 2 0 0 にシグナリングデータのトラヒック情報と帯域制御情報を設定しておき、ポリシーサーバが各 L A N デバイスに配信することで、各 L A N デバイスはシグナリングデータトラヒックに対して帯域制御を行う。また、ユーザデータに関しては以下に述べる手法により帯域制御を行う。

**【0024】**

移動端末 8 0 が発呼あるいは着呼した際に無線基地制御局 7 0 が送信する Q o S シグナリングを V P N ゲートウェイ 1 0 0 が受信し、V P N ゲートウェイ 1 0 0 が Q o S シグナリングに含まれるユーザデータのトラヒック情報を抽出し、トラヒック情報をポリシーサーバ 2 0 0 に通知する。ポリシーサーバ 2 0 0 がトラヒック情報に記載の帯域を許容できるか否かの受付判定を行う。ポリシーサーバ 2 0 0 が受付を許可した場合は、受付を許可した帯域制御情報及びトラヒック情報を移動通信トラヒックの経路上の L A N デバイス、あるいはすべての L A N デバイスに配信し、移動通信トラヒックの経路上の L A N デバイスはユーザデータトラヒックに対して通知された情報に基づき帯域制御を行う。

**【0025】**

次に、図 3 ~ 図 6 を参照して、本発明の第 1 の実施例に係る移動通信システムを構成する無線基地制御局 7 0、無線基地局 6 0、6 1、6 2、6 3、V P N ゲートウェイ 1 0 0 及びポリシーサーバ 2 0 0 の構成を説明する。

**【0026】**

無線基地制御局 7 0 は、例えば図 3 に示すような構成を備えている。具体的に説明すると、無線基地制御局 7 0 は、移動通信コア網側 I F 3 0 0 とインターネット側 I F 3 1 0 の 2 つのインタフェースを備え、L 2 処理部 3 2 0、4 1 0、I P トランスポート処理部 4 3 0、移動無線通信プロトコル処理部 3 3 0、移動無線通信制御部 3 6 0、帯域制御処理部 4 4 0 を備えて構成される。

**【0027】**

このうち、移動無線通信プロトコル処理部 3 3 0 の内部には、シグナリング処理部 3 4 0 とユーザデータ処理部 3 5 0 がある。I P トランスポート処理部 4 4 0 の内部には、I P 処理部 3 8 0、L 4 処理部 3 7 0、I P s e c 処理部 4 1 0 がある。I P s e c 処理部 4 1 0 は E S P (Encryption Security Payload) S A (Security Association) 情報 4 2 0 を保持する。これらの各処理部における基本的な処理を以下で説明する。

**【0028】**

移動通信コア網側 I F 3 0 0 から受信したシグナリングデータ及びユーザデータは、L

2 処理部 410 でリンク処理が行われた後、インターネット側 IF 310 から受信したシグナリングデータ及びユーザデータについては、L2 処理部 400、IP 処理部 380、L4 処理部 370 でそれぞれ規定の処理が行われた後、移動無線通信プロトコル処理部 330 において移動無線通信制御部 360 の制御に基づき規定の処理が行われる。

#### 【0029】

また、移動無線通信プロトコル処理部 330 がインターネット側 IF 310 からパケットを送信する場合、以下の手順で処理が行われる。

#### 【0030】

まず L4 処理部 370 において、シグナリングデータに対しては SCTP 処理が、ユーザデータに対しては UDP 処理が行われる。次に、IP 処理部 380 において、送信先の無線基地局 60 のオペレータ独自 IP アドレスを宛先、無線基地制御局 70 自身のオペレータ独自 IP アドレスを送信元とする内部 IP ヘッダが付加される。さらに、自身のグローバル IP アドレスを送信元、VPN ゲートウェイ 100 のグローバル IP アドレスを宛先とする外部 IP ヘッダでカプセル化される。その際、送信先の無線基地局 60 の SA 情報が ESP SA 情報 420 に含まれている場合には、IPsec 処理部 410 においてパケットが暗号化され、ESP ヘッダと ESP トレーラが付加される。

#### 【0031】

加えて、暗号化する際には、パケット内の L4 ヘッダをコピーして ESP ヘッダの前部に付加する。この理由は、LAN 20 の LAN デバイスがパケット識別する際に必要となる L4 ヘッダを閲覧できるようにするためである。

#### 【0032】

当該パケットは L2 処理部 410 においてリンク処理が行われた後、インターネット側 IF 310 から送信される。パケット受信時にはこれらの逆の処理が行われる。受信パケットに ESP ヘッダと ESP トレーラが含まれる場合には、IPsec 処理部 410 においてパケットの復号化が行われる。もし正しく復号できない場合には当該パケットは廃棄される。

#### 【0033】

IP トランスポート処理部 430 が送受信するパケットのフォーマットは、例えば図 7 の (b) に示すように構成される。図示するように、パケットは外部 IP ヘッダ 801、L4 ヘッダ 833、ESP ヘッダ 811、内部 IP ヘッダ 821、L4 ヘッダ 831、ペイロード 841、ESP トレーラ 851 から構成される。

#### 【0034】

図 1 に示した無線基地局 60 は、例えば図 4 に示すような構成を備えている。ここでは、無線基地局 60 を例にとって説明するが、無線基地局 61～63 も同様の構成を備えている。

#### 【0035】

具体的には、無線基地局 60 は、LAN 側 IF 500 と無線側 IF 510 の 2 つのインタフェースを有し、L2 処理部 520、移動無線通信プロトコル処理部 530、移動無線通信制御部 560、IP トランスポート処理部 630、Ethernet (R) 処理部 600 を備えて構成される。このうち、移動無線通信プロトコル処理部 530 の内部には、シグナリング処理部 540 と、ユーザデータ処理部 550 が備えられる。IP トランスポート処理部 630 には、L4 処理部 570、IP 処理部 580 と、IPsec 処理部 610 が備えられる。

#### 【0036】

IPsec 処理部 610 は ESP SA 情報 620 を保持する。これらの各処理部における基本的な処理を以下に示す。

#### 【0037】

無線側 IF 510 から受信したシグナリングデータ及びユーザデータは、L2 処理部 520 においてリンク処理が行われた後、LAN 側 IF 500 から受信したシグナリングデータ及びユーザデータについては、Ethernet (R) 処理部 600、IP 処理部 58

0、L4処理部570においてそれぞれ規定の処理が行われた後、移動無線通信プロトコル処理部530において移動無線通信制御部560の制御に基づき、規定の処理が行われる。

#### 【0038】

また、移動無線通信プロトコル処理部530が、LAN側IF500からパケットを送信する場合、以下の手順で処理が行われる。

#### 【0039】

まず、L4処理部570においてシグナリングデータにはSCTP処理を、ユーザデータにはUDP処理を行う。IP処理部580において送信先の無線基地制御局70のオペレータ独自IPアドレスを宛先、無線基地局60自身のオペレータ独自IPアドレスを送信元とする内部IPヘッダが付加される。また、送信元としては自身のプライベートIPアドレス、宛先としてはVPNゲートウェイ100のプライベートIPアドレスとする外部IPヘッダによるカプセル化も行われる。

#### 【0040】

その場合、送信先の無線基地局60のSA情報がESP SA情報620に含まれている場合には、IPsec処理部610がパケットの暗号化を行い、ESPヘッダとESPトレーラが付加される。加えて、暗号化する際に、L4ヘッダをコピーしてESPヘッダの前部に付加する。

#### 【0041】

当該パケットはEthernet(R)処理部600においてリンク処理された後、LAN側IF500から送信される。パケットを受信した場合はこの逆の処理が行われる。もし受信したパケットがESPヘッダとESPトレーラを含む場合は、IPsec処理部610においてパケットの復号化が行われる。正しく復号化できない場合には当該パケットは廃棄される。

#### 【0042】

IPトランスポート処理部630が送受信するパケットのフォーマットは、例えば図7の(a)に示すように構成される。図示するように、パケットは外部IPヘッダ800、L4ヘッダ832、ESPヘッダ810、内部IPヘッダ820、L4ヘッダ830、ペイロード840、ESPトレーラ850から構成される。

#### 【0043】

図1に示したVPNゲートウェイ100は例えば図5に示すような構成を備えている。

#### 【0044】

具体的には、VPNゲートウェイ100は、Global IP IF750及びPrivate IP IF700、Ethernet(R)処理部710、740、トンネル転送処理部720、IPsec処理部760から構成される。このうち、トンネル転送処理部720は経路制御情報730を保持し、IPsec処理部760はESP SA情報770を保持する。

#### 【0045】

図8～14を参照して、本発明の第1の実施例に係る移動通信システムを構成するVPNゲートウェイ100の動作内容について詳細に説明する。例えば、経路制御情報730は図8に示すような転送テーブル900から構成される。ここでは、転送テーブル900には、1つの無線基地制御局に関するグローバルアドレスとオペレータ独自アドレス、4つの無線基地局に関するプライベートアドレスとオペレータ独自アドレスが登録されている例を示している。

#### 【0046】

図9はVPNゲートウェイ100の全体の処理フローを示している。

#### 【0047】

VPNゲートウェイ100は、受信したパケットの外部IPヘッダ内の送信元IPアドレスがグローバルアドレスかプライベートアドレスかの判定を行う(ステップA-1)。プライベートアドレスの場合、受信パケットの種別の識別を行う(ステップA-2)。

**【0048】**

受信パケットが帯域制御応答である場合はQoSシグナリング処理を(ステップA-6)、アドレス通知である場合はアドレス通知パケット処理を(ステップA-5)行う。これらの処理の詳細については後述する。

**【0049】**

受信したパケットがIKEパケットである場合は送信元IPアドレスで転送テーブル900のプライベートアドレスを検索する(ステップA-4)。上記以外の場合は後述するIPsecパケット処理を行う(ステップA-3)。

**【0050】**

ステップA-4において該当するエントリが存在するかどうかを判別し(ステップA-7)、存在する場合、後述するIKEパケット転送処理を行い(ステップA-8)、該当するエントリが存在しなければ、受信パケットを廃棄する(ステップA-9)。

**【0051】**

一方、ステップA-1において外部IPヘッダ内の送信元IPアドレスがグローバルアドレスの場合、受信パケットの種別の識別を行う(ステップB-1)。受信パケットがIKEパケットである場合は送信元IPアドレスで転送テーブル900のグローバルアドレスを検索し(ステップB-3)、該当するエントリが存在するかを判定する(ステップB-4)。

**【0052】**

受信パケットがIKEパケット以外の場合は後述するIPsecパケット処理を行う(ステップB-2)。

**【0053】**

ステップB-4において該当するエントリが存在する場合、後述するIKEパケット転送処理を行い(ステップB-5)、該当するエントリが存在しない場合は、受信パケットを廃棄する(ステップB-6)。

**【0054】**

図10に、図9のステップA-5におけるアドレス通知パケット処理のフローを示す。この場合、送信元IPアドレスで転送テーブル900のプライベートアドレスを検索し(ステップC-1)、該当するエントリが存在するかどうかを判別する(ステップC-2)。

**【0055】**

該当するエントリが存在しない場合は、転送テーブル900に新たなエントリを追加し(ステップC-3)、処理を正常に完了したことを示すアドレス通知応答を送信する(ステップC-4)。該当するエントリが存在する場合はエラーを含むアドレス通知応答を返送する(ステップC-5)。

**【0056】**

図11にVPNゲートウェイ100によるSA情報の追加/削除処理のフローを示す。この場合、まず要求が追加か削除かの判定を行う(ステップD-1)。

**【0057】**

追加要求である場合、メッセージ内に含まれるIPアドレス、IPsecプロトコル種別及びSPI(Security Parameter Index)のすべてが同一であるエントリが存在するかをチェックする(ステップD-2)。該当するエントリが存在しない場合、SA情報のエントリを新たに追加し(ステップD-3)、SA情報追加応答を返信する(ステップD-4)。ステップD-2において該当するエントリが存在する場合は、SA情報追加応答(エラー)を返信する(ステップD-5)。

**【0058】**

削除要求である場合、追加処理と同様にメッセージ内の情報と同一のエントリが存在するかをチェックする(ステップD-6)。該当するエントリが存在する場合、SA情報のエントリを削除し(ステップD-7)、SA情報削除応答を返信する(ステップD-8)。ステップD-6において該当するエントリが存在しない場合、SA情報削除応答(エラ

一)を返信する(ステップD-9)。

【0059】

図12に、図9のステップA-3、B-2におけるVPNゲートウェイ100によるIPsecパケット処理のフローを示す。

【0060】

この場合、まずパケットを受信したIFの判定を行う(ステップE-1)。

【0061】

プライベートIFでパケットを受信した場合、ESPヘッダ内のSPIでSA情報を検索してマッチするエントリが存在するかを判定する(ステップE-2、E-3)。

【0062】

該当するエントリが存在しない場合はパケットを廃棄する(ステップE-4)。該当するエントリが存在する場合、該当のSA情報に基づきパケットの復号化を行い(ステップE-5)、内部IPヘッダ及びL4ヘッダの情報でSA情報の該当するエントリを検索してマッチするエントリが存在するかを判定する(ステップE-6、E-7)。該当するエントリが存在しない場合はパケットを廃棄する(ステップE-8)。

【0063】

該当するエントリが存在する場合、該当するSA情報に基づき暗号化を行い(ステップE-9)、SA情報のトンネル終端先IPアドレスを宛先とするIPヘッダに置き換えて、カプセル化転送を行う(ステップE-10)。

【0064】

一方、グローバルIFでパケットを受信した場合、ESPヘッダ内のSPIでSA情報を検索しマッチするエントリが存在するかを判定する(ステップE-11、E-12)。

【0065】

該当するエントリが存在しない場合はパケットを廃棄する(ステップE-13)。該当するエントリが存在する場合は、該当するSA情報に基づきパケットの復号化を行い(ステップE-14)、パケット種別をチェックする(ステップE-15)。

【0066】

QoSシグナリングの場合、後述するQoSシグナリング処理を行い(ステップE-16)、SA情報追加/削除要求である場合、図11に示したSA情報追加/削除処理を行う(ステップE-17)。

【0067】

ステップE-15においてパケット種別が上記以外の場合、内部IPヘッダ及びL4ヘッダの情報でSA情報の該当するエントリを検索し、マッチするエントリが存在するかを判定する(ステップE-18、E-19)。

【0068】

該当するエントリが存在しない場合はパケットを廃棄する(ステップE-20)。該当するエントリが存在する場合、該当するSA情報に基づきパケットの暗号化を行い(ステップE-21)、SA情報のトンネル終端先IPアドレスを宛先とする外部IPヘッダに置き換えて、カプセル化転送を行う(ステップE-22)。

【0069】

図13に図9のステップA-8、B-5におけるVPNゲートウェイ100によるIKEパケット転送処理のフローを示す。

【0070】

この場合、まずパケットを受信したインタフェース(IF)の判定を行う(ステップF-1)。

【0071】

受信IFがプライベートIFである場合、送信元IPアドレスで転送テーブル900のプライベートアドレスを検索し、マッチするエントリが存在するかを判定する(ステップF-2、F-3)。

【0072】

該当するエントリが存在しない場合は、パケットを廃棄する（ステップF-4）。

【0073】

該当するエントリが存在する場合、外部IPヘッダを削除し（ステップF-5）、該当するエントリに記載のグローバルアドレスを宛先とするIPヘッダを付加して、カプセル化転送を行う（ステップF-6）。

【0074】

一方、ステップF-1において受信IFがグローバルIFである場合、送信元IPアドレスで転送テーブル900のグローバルアドレスを検索し、マッチするエントリが存在するかを判定する（ステップF-7、F-8）。

【0075】

該当するエントリが存在しない場合はパケットを廃棄する（ステップF-9）。該当するエントリが存在する場合、内部IPヘッダ内の宛先IPアドレスで転送テーブル900の無線基地局のオペレータ独自アドレスを検索し、マッチするエントリが存在するかを判定する（ステップF-10、F-11）。

【0076】

該当するエントリが存在しない場合はパケットを廃棄する（ステップF-12）。該当するエントリが存在する場合、外部IPヘッダを削除し（ステップF-13）、該当するエントリに記載のプライベートアドレスを宛先とするIPヘッダを付加して、カプセル化転送を行う（ステップF-14）。

【0077】

図14に、図9のステップA-6におけるVPNゲートウェイ100によるQoSシグナリング処理の動作フローを示す。

【0078】

この場合も、まずパケットの受信IFの判定を行う（ステップG-1）。

【0079】

受信IFがプライベートIFの場合、受信した帯域制御応答（COPS Decision）メッセージ内部の受付判定結果をチェックする（ステップG-2）。

【0080】

判定結果が「NG」の場合は判定結果とトラヒック情報を含むQoSシグナリングを作成し、無線基地制御局70に送信する（ステップG-3）。

【0081】

判定結果が「OK」の場合、帯域制御応答メッセージで通知されたトラヒック情報及び帯域制御情報を抽出し（ステップG-4）、抽出した各種情報をQoSシグナリングに含めて、無線基地制御局70に送信する（ステップG-5）。

【0082】

一方、ステップG-1において受信IFがグローバルIFの場合、QoSシグナリング内のトラヒック情報を抽出し（ステップG-6）、抽出したトラヒック情報を含む帯域制御要求（COPS Request）メッセージを作成し、ポリシーサーバ200に送信する（ステップG-7）。

【0083】

ポリシーサーバ200は、例えば図6に示すような構成を備えている。具体的に説明すると、ポリシーサーバ200は、LAN IF1300、Ethernet(R)処理部1310、IP処理部1320、L4処理部1330、制御プロトコル処理部1340、帯域制御処理部1350を備えて構成される。制御プロトコル処理部1340は、COPS処理部1360とSNMP処理部1370を有する。これらの各処理部の基本的な処理内容を以下に示す。

【0084】

SNMP処理部1370は、LAN IF1300、Ethernet(R)処理部1310、IP処理部1320、L4処理部1330を経て受信した、LAN20のLANデバイスからのSNMPメッセージを受信し、メッセージ内の帯域制御状態情報を抽出し、

帯域制御処理部1350に通知する。

【0085】

帯域制御処理部1350は、これらの情報を収集／管理し、LAN20内の帯域制御状態を集中管理する。

【0086】

COPS処理部1360は、帯域制御処理部1350からの指示を受けることにより、LANデバイスに対して帯域制御情報及びトラヒック情報をCOP Decisionメッセージで通知する。

【0087】

また、VPNゲートウェイ100から送られた帯域制御要求メッセージは、LAN IF1300、Ethernet(R)処理部1310、IP処理部1320、L4処理部1330を経てCOPS処理部1360に送られ、COPS処理部1360が帯域制御要求メッセージ内のトラヒック情報と帯域制御情報を抽出し、帯域制御処理部1350に通知する。

【0088】

これを受けた帯域制御処理部1350は、収集した帯域制御情報に基づき受付判定を行い、許可した帯域制御情報と共に判定結果をCOPS処理部1360に通知する。判定結果が「OK」であった場合には、COPS処理部1360は判定結果と許可された帯域制御情報を含む帯域制御応答メッセージを生成し、VPNゲートウェイ100に送信する。また、LAN20の移動通信トラヒックの経路上のLANデバイスあるいはすべてのLANデバイスにトラヒック情報と帯域制御情報を配信する。

【0089】

図15を参照して、本発明の第1の実施形態に係る移動通信システムにおける無線基地制御局70と無線基地局60間で通信経路を確立するための動作シーケンスについて詳細に説明する。図15においては、無線基地局60の送受信パケットシーケンス1000、VPNゲートウェイ100の送受信パケットシーケンス1010、及び無線基地制御局70の送受信パケットシーケンス1020を示している。

【0090】

本実施例では、VPNゲートウェイ100と無線基地制御局70間には予めSAが確立されており、無線基地局60とVPNゲートウェイ100間でSAを確立する際に必要となる事前共有鍵は、無線基地制御局70と無線基地局60に予め設定されているものとする。

【0091】

以下では、より詳細な動作シーケンスを説明する。無線基地局60は起動すると、DHCP(Dynamic Host Configuration Protocol)により自身のプライベートIPアドレスを取得した後、DNS(Domain Name Server)を利用してVPNゲートウェイ100のプライベートIPアドレスを取得する。

【0092】

その後、VPNゲートウェイ100に対して、無線基地制御局70のグローバルアドレスとオペレータ独自アドレス、無線基地局60のプライベートアドレスとオペレータ独自アドレスをアドレス通知メッセージで通知する。

【0093】

VPNゲートウェイ100はこれを受けて、転送テーブル900に通知されたアドレス群を設定し、設定したエントリを削除するためのタイマをセットすると共に、アドレス通知応答メッセージを返信する(ステップ(1))。

【0094】

返信メッセージを受けた無線基地局60は、VPNゲートウェイ100とのISAKMP SA及び上りと下りの2つのIPsec SAを確立する(ステップ(2)～(4))。その場合、VPNゲートウェイ100は無線基地局60から受信したIKEパケットのアドレス変換のみを行い、無線基地制御局70に転送する。

## 【0095】

逆に、無線基地制御局 70 から受信した I K E パケットもアドレス変換のみを行い、無線基地局 60 に転送する。

## 【0096】

このようにして無線基地制御局 70 と無線基地局 60 間で S A が確立されると、無線基地制御局 70 はすべての S A 情報を S A 情報追加メッセージにて V P N ゲートウェイ 100 に通知する。

## 【0097】

V P N ゲートウェイ 100 は、受信した S A 情報をデータベースに追加し、ステップ (1) でセットしたタイマを解除すると共に、S A 情報追加応答メッセージにて設定が完了したことを通知する (ステップ (5))。

## 【0098】

これにより、V P N ゲートウェイ 100 と無線基地局 60 間では I P s e c による暗号化通信が可能となり、V P N ゲートウェイ 100 を介することで無線基地局 60 と無線基地制御局 70 は I P s e c S A による暗号化通信を開始できる (ステップ (6))。

## 【0099】

もし、V P N ゲートウェイ 100 が S A 情報追加メッセージを受信せずに、タイマがタイムアウトした際には、速やかに追加した転送テーブル 900 のエントリを削除する。

## 【0100】

図 16 及び図 17 を参照して、本発明の第 1 の実施例に係る移動通信システムにおける無線基地制御局 70 と無線基地局 60 間のユーザトラヒックに対する帯域制御動作シーケンスを詳細に説明する。

## 【0101】

図 16 に端末が着呼した場合の動作シーケンスを示す。図 16 においては、無線基地制御局 70 のパケット送受信シーケンス 1100、V P N ゲートウェイ 100 のパケット送受信シーケンス 1110、ポリシーサーバ 200 のパケット送受信シーケンス 1120、無線基地局 60 のパケット送受信シーケンス 1130、移動端末 80 のパケット送受信シーケンス 1140 を示している。

## 【0102】

無線基地制御局 70 は、移動通信コア網 30 からのページング要求メッセージを受信すると (ステップ (1))、移動端末 80 のページングを行い (ステップ (2))、これに対して移動端末 80 は R R C コネクション要求を無線基地制御局 70 に送信し (ステップ (3))、これを受信した無線基地制御局 70 は無線基地局 60 に対して無線リンク設定要求を送信する (ステップ (4))。

## 【0103】

無線リンクの設定を完了すると、無線基地局 60 は、無線基地制御局 70 に無線リンク設定応答を返送し (ステップ (5))、無線基地制御局 70 は、R R C コネクション設定を移動端末 80 に送信する (ステップ (6))。

## 【0104】

これを受けた移動端末 80 は、各種パラメータを設定した後、R R C コネクション設定完了を無線基地制御局 70 に送信する (ステップ (7))。その後、移動端末 80 は、セルアップデータメッセージにより位置登録を行う (ステップ (8))。

## 【0105】

これを受けた無線基地制御局 70 は、セルアップデート確認メッセージで返信すると共に (ステップ (9))、ページング応答を移動通信コア網 30 に返送する (ステップ (10))。この後、無線基地制御局 70 は、移動通信コア網 30 から送られた無線アクセスベアラ割当要求メッセージを受信し (ステップ (11))、無線ベアラ確立要求メッセージに含まれる Q o S 情報に基づき、無線リンクの設定を行う。

## 【0106】

具体的には、無線基地制御局 70 は、無線基地局 60 に無線リンク設定要求を送信し (



ステップ(12))、無線基地局60は無線リンクの設定が完了すると無線リンク設定応答を返信する(ステップ(13))。

**【0107】**

これを受けた無線基地制御局70は、要求されたQoSの情報を含むQoSシグナリングを生成し、無線基地局60に送信する(ステップ(14))。

**【0108】**

VPNゲートウェイは、このQoSシグナリングをインターセプトし、QoSシグナリングから抽出したトラフィック情報を含む帯域制御要求メッセージをポリシーサーバ200に送信する(ステップ(15))。ここでのQoSシグナリングとは、例えばIP-ALCAP (Access Link Control Application Part)シグナリングである。

**【0109】**

ポリシーサーバ200は、収集した帯域制御状態情報と帯域制御要求メッセージで通知されたトラフィック情報に基づき受付判定を行い、受付判定結果及び許可した帯域制御情報を帯域制御応答メッセージに含めてVPNゲートウェイ100に送信する通知する(ステップ(16))。

**【0110】**

VPNゲートウェイ100は、帯域制御応答メッセージに含まれる受付判定結果と帯域制御情報をQoSシグナリングに含めて無線基地制御局70に送信する(ステップ(17))。本実施例ではポリシーサーバ200が受付許可と判定した例を示している。

**【0111】**

受付を許可した場合、ポリシーサーバ200は、LAN20のLANデバイスにトラフィック情報と帯域制御情報の配布も行う(図示せず)。LAN内の帯域確保が完了すると、無線基地制御局70は、移動端末80に無線ベアラ設定を送信する(ステップ(18))。

。

**【0112】**

これを受信した移動端末80は、無線ベアラの設定を行い、完了すると無線ベアラ設定完了を返信する(ステップ(19))。その後、移動端末80は、無線基地制御局70及び移動通信コア網30を経由してデータ通信を行う。LAN20の移動通信トラフィックの経路上にあるLANデバイスは、通知されたトラフィック情報と帯域制御情報に基づいてユーザデータトラフィックの帯域制御が行う。

**【0113】**

図17に移動端末80が発呼した場合の動作シーケンスを示す。図17においては、無線基地制御局70の packets 送受信シーケンス1200、VPNゲートウェイ100の packets 送受信シーケンス1210、ポリシーサーバ200の packets 送受信シーケンス1220、無線基地局60の packets 送受信シーケンス1230、移動端末80の packets 送受信シーケンス1240を示している。

**【0114】**

移動端末80は、データの送信要求をトリガとしてRRCコネクション要求を無線基地制御局70に送信する(ステップ(1))。これを受信した無線基地制御局70は、無線基地局60へ無線リンク設定要求を送信する(ステップ(2))。無線基地局60は、無線リンクの設定を有効化し、無線基地制御局70に無線リンク設定応答を返す(ステップ(3))。

**【0115】**

無線基地局60からの無線リンク設定応答を受信した無線基地制御局70は、RRCコネクション設定を移動端末80に送信し(ステップ(4))、移動端末80は、無線リンクの設定が完了すると、RRCコネクション設定完了を無線基地制御局70に送信する(ステップ(5))。また、移動端末80は、利用するサービスのQoS情報を含むアクティベートPDPコンテキスト要求を移動通信コア網30に送信する(ステップ(6))。

**【0116】**

これを受けて、移動通信コア網30は、無線アクセスベアラ割当要求を無線基地制御局

70に送信する(ステップ(7))。無線基地制御局70は、無線アクセスベアラ割当要求に含まれるQoS情報に基づき、無線リンクの設定を行う。具体的には、無線基地制御局70は、無線基地局60に無線リンク設定要求を送信し(ステップ(8))、無線基地局60が無線リンクの設定を完了すると、無線リンク設定応答を返送する(ステップ(9))。

#### 【0117】

これを受けて、無線基地制御局70は、QoS情報を含むQoSシグナリングを生成し、無線基地局60宛に送信する(ステップ(10))。VPNゲートウェイ100は、このQoSシグナリングをインターセプトし、受信したQoSシグナリングから抽出したQoS情報を含む帯域制御要求メッセージをポリシーサーバ200に送信する(ステップ(11))。

#### 【0118】

ポリシーサーバ200は、収集した帯域制御状態情報と帯域制御要求メッセージで通知されたQoS情報に基づき受付判定を行い、受付判定結果及び許可した帯域制御情報を帯域制御応答メッセージに含めてVPNゲートウェイ100に送信する通知する(ステップ(12))。

#### 【0119】

VPNゲートウェイ100は、帯域制御応答メッセージに含まれる受付判定結果と帯域制御情報をQoSシグナリングに含めて無線基地制御局70に送信する(ステップ(13))。本実施例でもポリシーサーバ200が受付許可と判定した例を示している。

#### 【0120】

受付を許可した場合、ポリシーサーバ200は、LAN20のLANデバイスにトラヒック情報と帯域制御情報を配布する(図示せず)。その後、無線基地制御局70は移動端末80に対して無線ベアラ設定を通知する(ステップ(14))。

#### 【0121】

移動端末80は、無線リンクの設定を行い、完了すると無線ベアラ設定完了を無線基地制御局70に通知する(ステップ(15))。これを受けて、無線基地制御局70は、無線アクセスベアラ割当応答を移動通信コア網30に返送する(ステップ(16))。

#### 【0122】

移動端末80は、移動通信コア網30からアクティベートPDPコンテキスト受付を受信する(ステップ(17))と、無線基地制御局70及び移動通信コア網30を経由してデータ通信を行う。LAN20の移動通信トラヒックの経路上にあるLANデバイスは通知されたトラヒック情報と帯域制御情報に基づいてユーザデータトラヒックの帯域制御を行う。

#### 【0123】

図1及び2に示すネットワーク構成図を用いて本発明の第2の実施例に係わる移動通信システムを説明する。この第2の実施例では、無線基地制御局70は、例えば図18に示す構成を備えている。

#### 【0124】

第1の実施形態での無線基地制御局70の構成と比較して、本第2の実施例では、IPトランスポート処理部430がIP処理部380、L4処理部370、IPsec処理部410に加えて、認証処理部450を備えている。

#### 【0125】

認証処理部450は、無線基地局60～63との間で認証を行うと共に、認証が成功した場合には、鍵交換メカニズムを用いて事前共有鍵の生成も行う。無線基地制御局70は、SAが確立すると、生成した事前共有鍵をVPNゲートウェイ100に通知する。VPNゲートウェイ100は、この事前共有鍵を用いて無線基地局60～63と間でIPsec SAの確立を行う。

#### 【0126】

無線基地局60は、例えば図19に示す構成を備える。ここでの実施例では無線基地局

60について説明するが、無線基地局61～63についても同様の構成を備えている。第1の実施形態での無線基地局60の構成と比較して、本実施例では、IPトランスポート処理部630がIP処理部580、L4処理部570、IPsec処理部610に加えて、認証処理部640を備えている。認証処理部640は、無線基地制御局70との間で認証を行うために、上述した認証処理部450と同様の機能を有する。

#### 【0127】

図20～22を用いてVPNゲートウェイ100の動作フローを説明する。

#### 【0128】

図20に全体の処理フローを示す。まず、パケットを受信することで処理を開始し、受信したパケットの種別を判定する(ステップH-1)。受信したパケットがIPsecパケットであった場合、後述するIPsecパケット処理を行う(ステップH-2)。IKEパケットであった場合、RFC2409で規定されているIKEパケット処理を行う(ステップH-3)。認証パケットであった場合、後述する認証パケット転送処理を行う(ステップH-4)。帯域制御応答メッセージであった場合、QoSシグナリング処理を行う(ステップH-5)。ここでのQoSシグナリング処理は第1の実施形態で示したQoSシグナリング処理と同様である。受信したパケットが上記以外の場合はパケットを廃棄する(ステップH-6)。

#### 【0129】

図21に、上記ステップH-2におけるVPNゲートウェイ100のIPsecパケット処理のフローを示す。第1の実施形態で示した図12のIPsecパケット処理では、グローバルIFからパケットを受信し、ESPヘッダ内のSPIでSA情報を検索した際に、該当するエントリが存在し、且つパケット種別がSA情報追加/削除要求である場合には、ステップE-17でSA情報追加/削除処理を行うようにしていたが、本実施例では、パケット種別がSA情報追加/削除要求ではなく、認証パケットである場合に、SA情報追加/削除処理の代わりに認証パケット転送処理を行う(ステップI-17)点で第1の実施例と異なる。

#### 【0130】

その他のステップについては、図12と同様であるので、同じステップ番号を付して説明を省略する。

#### 【0131】

図22に図21のステップI-17における認証パケット転送処理のフローを示す。この場合、まずパケットを受信したIFの判定を行う(ステップJ-1)。

#### 【0132】

受信IFがプライベートIFの場合、内部IPヘッダのSPIでSA情報を検索し、マッチするエントリが存在するかを判定する(ステップJ-2、J-3)。

#### 【0133】

該当するエントリが存在しない場合はパケットを廃棄する(ステップJ-4)。

#### 【0134】

該当するエントリが存在する場合、該当するSA情報に基づき復号化を行い(ステップJ-5)、SA情報のトンネル終端先のIPアドレスでカプセル化して転送する(ステップJ-6)。

#### 【0135】

一方、ステップJ-1において受信IFがグローバルIFの場合、事前共有鍵通知メッセージであるかの判定を行う(ステップJ-7)。

#### 【0136】

事前共有鍵通知メッセージである場合、メッセージ内の事前共有鍵を抽出し、IPsec処理部760に通知する(ステップJ-8)。

#### 【0137】

それ以外の場合、内部IPヘッダの宛先IPアドレスで転送テーブル900を検索し、マッチするエントリが存在するかを判定する(ステップJ-9、J-10)。

## 【0138】

該当するエントリが存在しない場合はパケットを廃棄する（ステップJ-11）。該当するエントリが存在する場合は、該当するエントリのプライベートアドレスでカプセル化して転送する（ステップJ-12）。

## 【0139】

また、図23を参照して、本発明の第2の実施例に係る移動通信システムにおける無線基地制御局70と無線基地局60間で通信経路を確立するための動作シーケンスを詳細に説明する。

## 【0140】

第2の実施例では、無線基地局60と無線基地制御局70間の相互認証で使用する認証鍵が予め設定されており、無線基地制御局70とVPNゲートウェイ100の間のSAは事前に確立されているものとする。また、VPNゲートウェイ100が有する転送テーブル900も予め設定されているものとする。図23においては、無線基地局60のパケット送受信シーケンス1400、VPNゲートウェイ100のパケット送受信シーケンス1410、及び無線基地制御局70のパケット送受信シーケンス1420が示されている。

## 【0141】

無線基地局60は起動すると、事前に設定されている認証鍵を用いて、無線基地制御局70との間で相互認証を行う（ステップ（1））。ここでの認証方式は、例えば認証鍵を利用したチャレンジ/レスポンス型のワンタイムパスワード方式が利用可能である。

## 【0142】

相互認証が成功した場合、無線基地局60と無線基地制御局70において鍵交換メカニズムにより認証鍵から事前共有鍵の生成を行う（ステップ（2））。ここでの鍵交換メカニズムとしては、例えばDiffie-Hellman鍵交換方式が利用可能である。

## 【0143】

鍵の生成が完了すると、無線基地制御局70はVPNゲートウェイ100に対して事前共有鍵を通知する（ステップ（3））。

## 【0144】

無線基地局60は上述した鍵交換メカニズムにより生成した事前共有鍵を用いてISAKMP SAの確立を行う（ステップ（4））。

## 【0145】

ISAKMP SAを確立すると、次にIPsec SA（上り）とIPsec SA（下り）の確立も行う（ステップ（5）、（6））。

## 【0146】

上り／下りの2つのIPsec SAが確立すると、無線基地局60と無線基地制御局70はVPNゲートウェイ100を介することで、IPsec ESPによる暗号化通信が可能となる（ステップ（7））。

## 【0147】

なお、上記の構成において、VPNゲートウェイ100、無線基地制御局70の機能については、ハードウェア的に実現することは勿論として、上記したVPNゲートウェイ100の機能をソフトウェア的に実現するプログラム（中継ノード用プログラム）、無線基地制御局70の機能をソフトウェア的に実現する制御プログラム（無線基地制御局用プログラム）を、それぞれVPNゲートウェイ100、無線基地制御局70を構成するコンピュータ処理装置上で実行することで実現することができる。これらのプログラムは、磁気ディスク、半導体メモリその他の記録媒体に格納され、その記録媒体からVPNゲートウェイ100、無線基地制御局70としてのコンピュータ処理装置にロードされ、コンピュータ処理装置の動作を制御することにより、上述した各機能を実現する。

## 【0148】

以上好ましい実施例をあげて本発明を説明したが、本発明は必ずしも上記実施例に限定されるものではなく、その技術的思想の範囲内において様々に変形して実施することができる。

## 【図面の簡単な説明】

【0149】

【図1】本発明の第1の実施例によるネットワークの全体構成を示すブロック図である。

【図2】本発明の第1の実施例におけるLANの構成を示すブロック図である。

【図3】本発明の第1の実施例における無線基地制御局の構成を示すブロック図である。

【図4】本発明の第1の実施例における無線基地局の構成を示すブロック図である。

【図5】本発明の第1の実施例におけるVPNゲートウェイの構成を示すブロック図である。

【図6】本発明の第1の実施例におけるポリシーサーバの構成を示すブロック図である。

【図7】本発明の第1の実施例における転送テーブルの構成例を示す図である。

【図8】本発明の第1の実施例におけるパケットフォーマットの構成を示す図である。

【図9】本発明の第1の実施例におけるVPNゲートウェイにおける全体処理を説明するフローチャートである。

【図10】本発明の第1の実施例におけるVPNゲートウェイのアドレス通知処理を説明するフローチャートである。

【図11】本発明の第1の実施例におけるVPNゲートウェイのSA情報追加／削除処理を説明するフローチャートである。

【図12】本発明の第1の実施例におけるVPNゲートウェイのIPsecパケット処理を説明するフローチャートである。

【図13】本発明の第1の実施例におけるVPNゲートウェイのIKEパケット処理を説明するフローチャートである。

【図14】本発明の第1の実施例におけるVPNゲートウェイにおけるQoSシグナリング処理を説明するフローチャートである。

【図15】本発明の第1の実施例における無線基地制御局と無線基地局間の通信開始シーケンス図である。

【図16】本発明の第1の実施例における着呼時の帯域制御動作のシーケンス図である。

【図17】本発明の第1の実施例における発呼時の帯域制御動作のシーケンス図である。

【図18】本発明の第2の実施例における無線基地制御局の構成を示すブロック図である。

【図19】本発明の第2の実施例における無線基地局の構成を示すブロック図である。

【図20】本発明の第2の実施例におけるVPNゲートウェイの全体処理を説明するフローチャートである。

【図21】本発明の第2の実施例を説明するためのVPNゲートウェイにおけるIPsecパケット処理フロー図である。

【図22】本発明の第2の実施例におけるVPNゲートウェイの認証パケット転送処理を説明するフローチャートである。

【図23】本発明の第2の実施例における無線基地制御局と無線基地局間の通信開始シーケンス図である。

## 【符号の説明】

【0150】

10: インターネット網

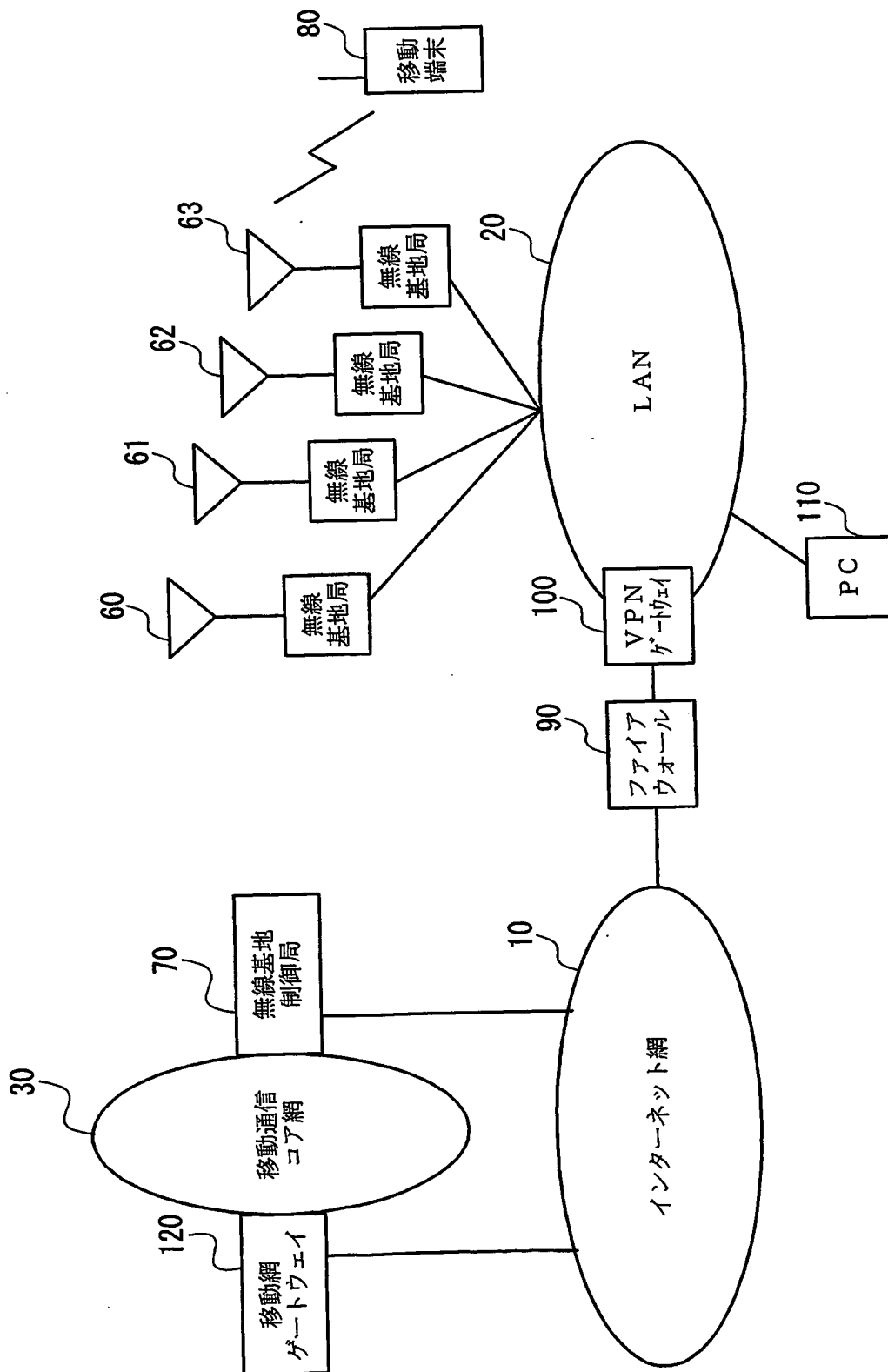
20: LAN

30: 移動通信コア網

60、61、62、63:無線基地局  
70:無線基地制御局  
80:移動端末  
90:ファイアウォール  
100:VPNゲートウェイ  
110:PC  
120:移動網ゲートウェイ  
200:ポリシーサーバ  
210:ルータ  
220~223:Ethernet(R)スイッチ  
300:移動通信コア網側IF  
310:インターネット側IF  
320、400、520:L2処理部  
330、530:移動無線通信プロトコル処理部  
340、540:シグナリング処理部  
350、550:ユーザデータ処理部  
360、560:移動無線通信制御部  
370、570:L4処理部  
380、580:IP処理部  
410、610、760:IPsec処理部  
420、620、770:ESP SA情報  
430、630:IPトランスポート処理部  
440、780:帯域制御処理部  
450、640:認証処理部  
500:LAN側IF  
510:無線側IF  
600、710、740:Ethernet(R)処理部  
700:プライベートIP IF  
720:トンネル転送処理部  
730:経路制御情報  
750:グローバルIP IF  
800、801:外部IPヘッダ  
810、811:ESPヘッダ  
820、821:内部IPヘッダ  
830、831:L4ヘッダ  
840、841:ペイロード  
850、851:ESPトレーラ  
900:転送テーブル  
1000、1130、1230、1400:無線基地局の packets 送受信シーケンス  
1010、1110、1210、1410:VPNゲートウェイの packets 送受信シーケンス  
1020、1100、1200、1420:無線基地制御局の packets 送受信シーケンス  
1120、1220:ポリシーサーバの packets 送受信シーケンス  
1140、1240:移動端末の packets 送受信シーケンス  
1300:LAN IF  
1310:Ethernet(R)処理部  
1320:IP処理部  
1330:L4処理部  
1340:制御プロトコル処理部

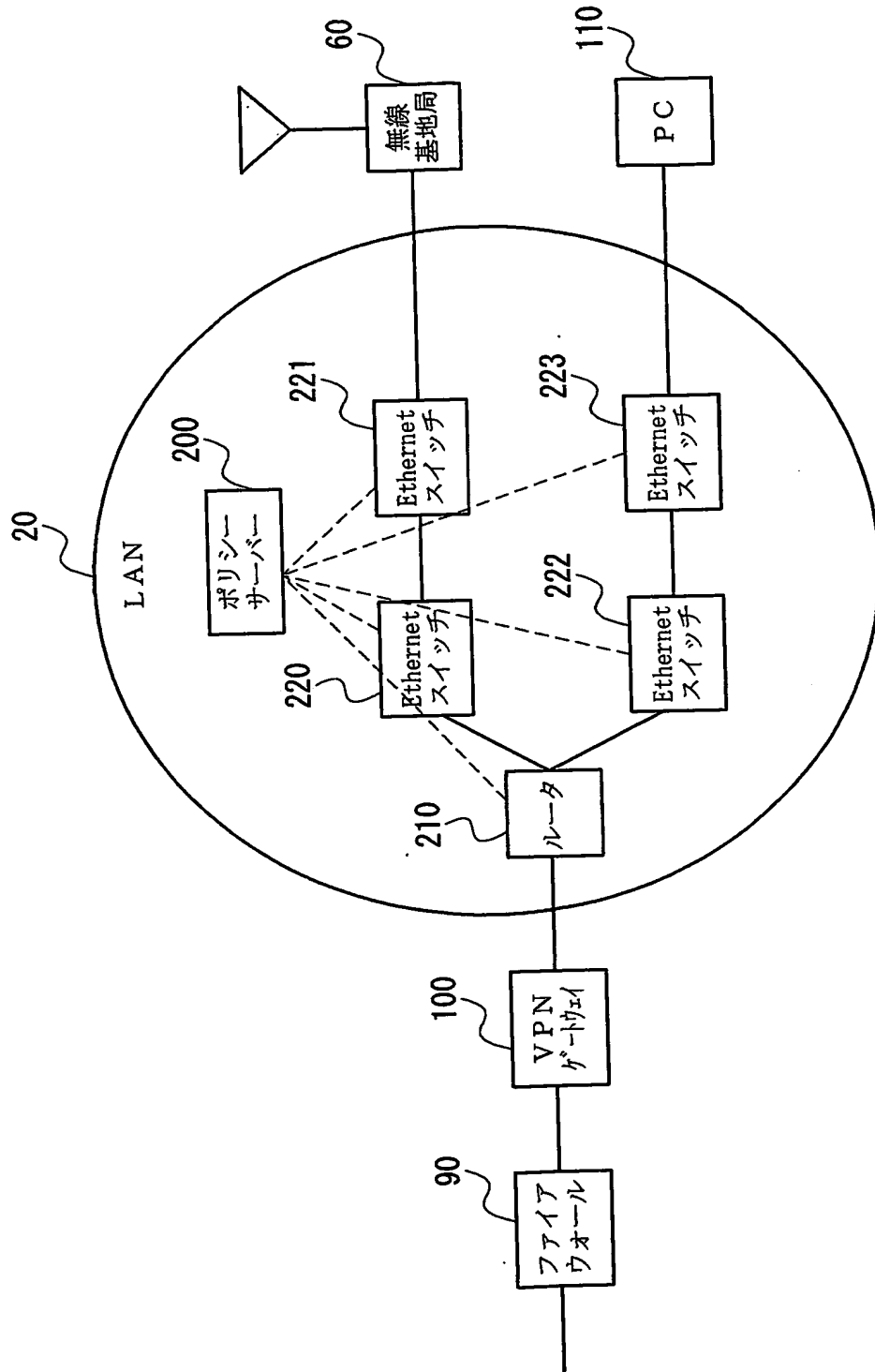
1 3 5 0 : 帯域制御処理部  
1 3 6 0 : C O P S 処理部  
1 3 7 0 : S N M P 処理部

【書類名】 図面  
【図 1】

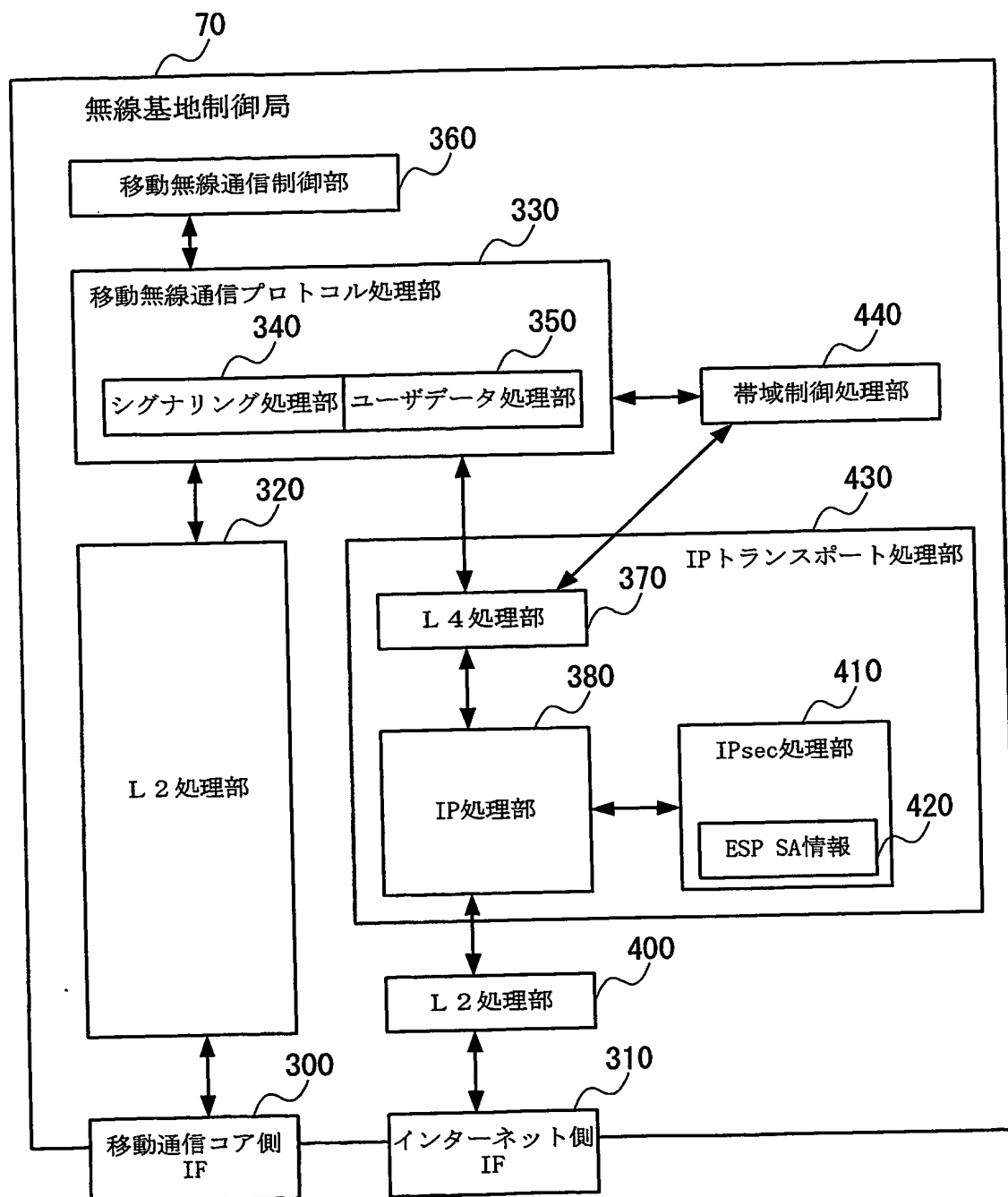




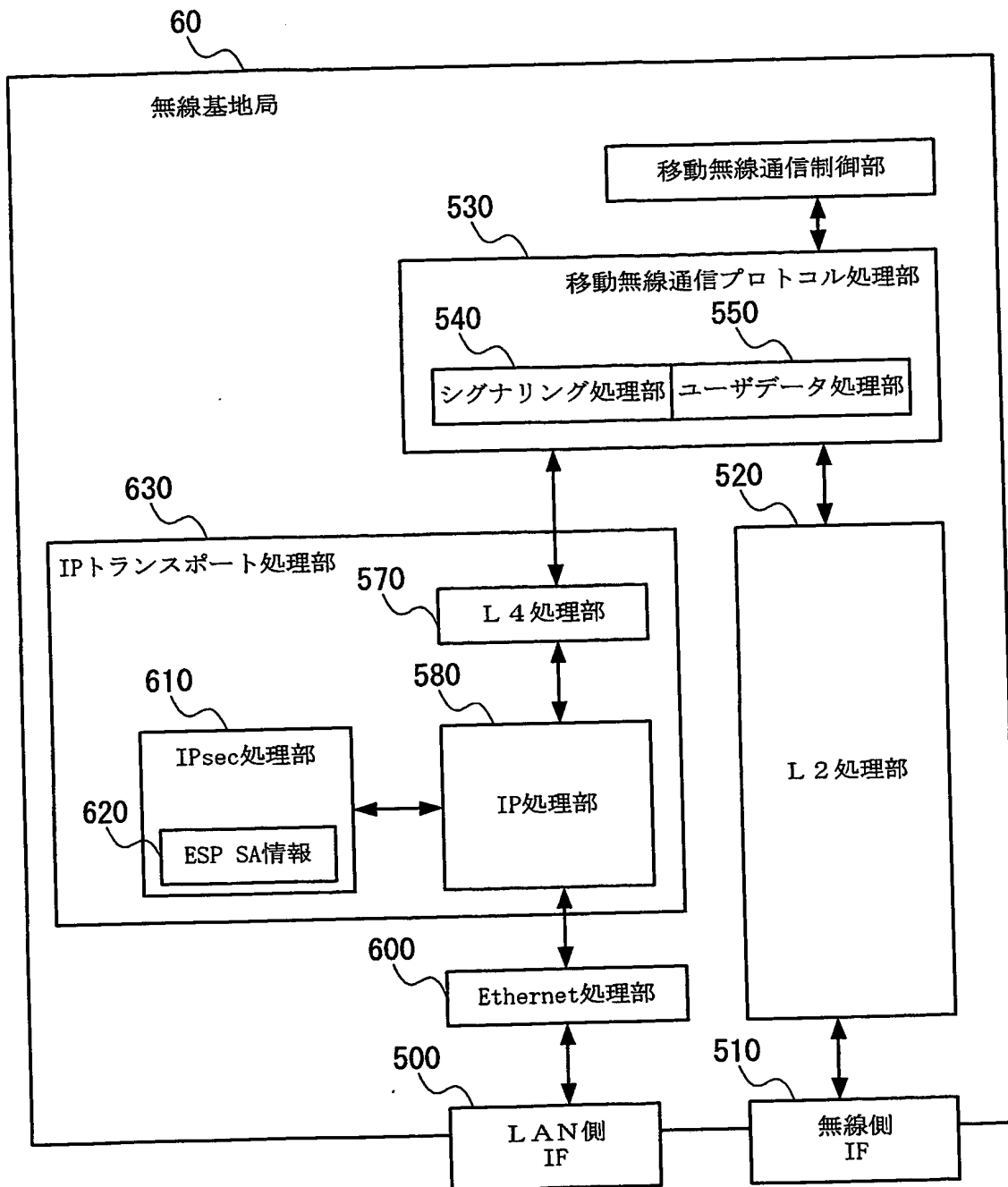
【図 2】



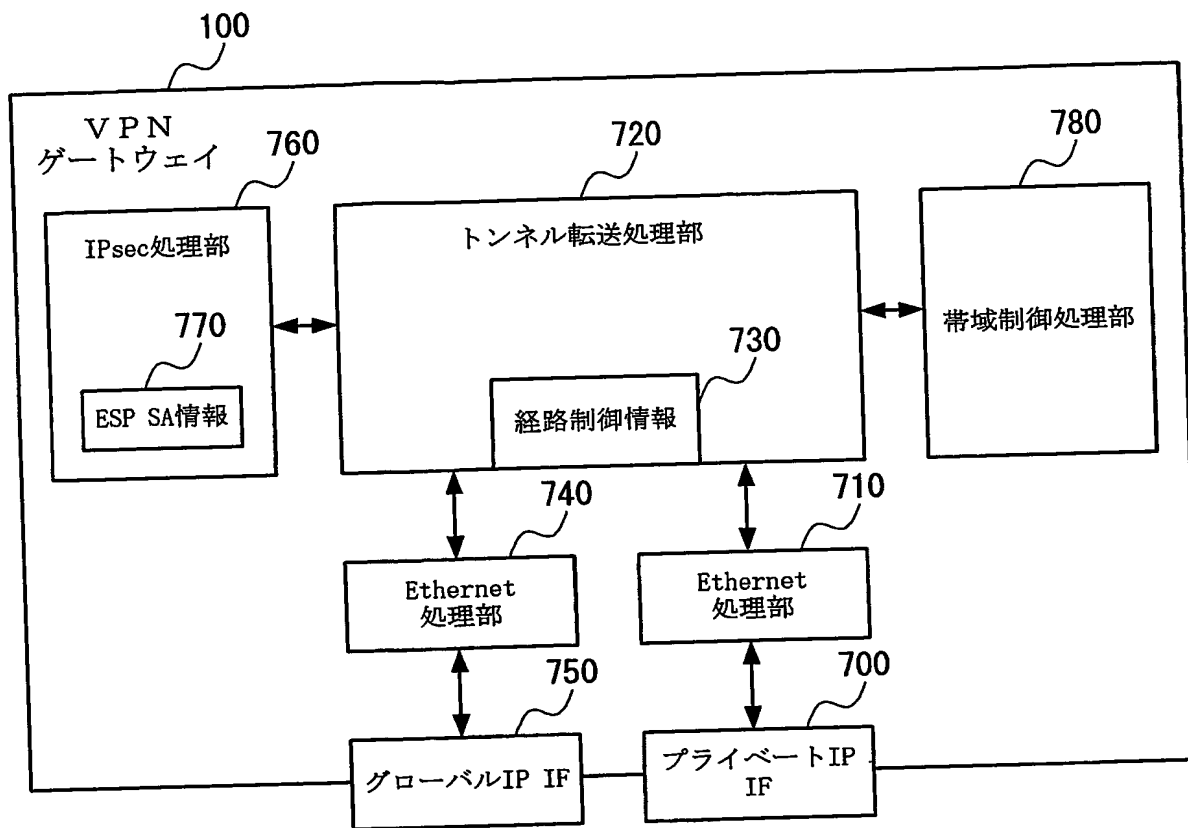
【図 3】



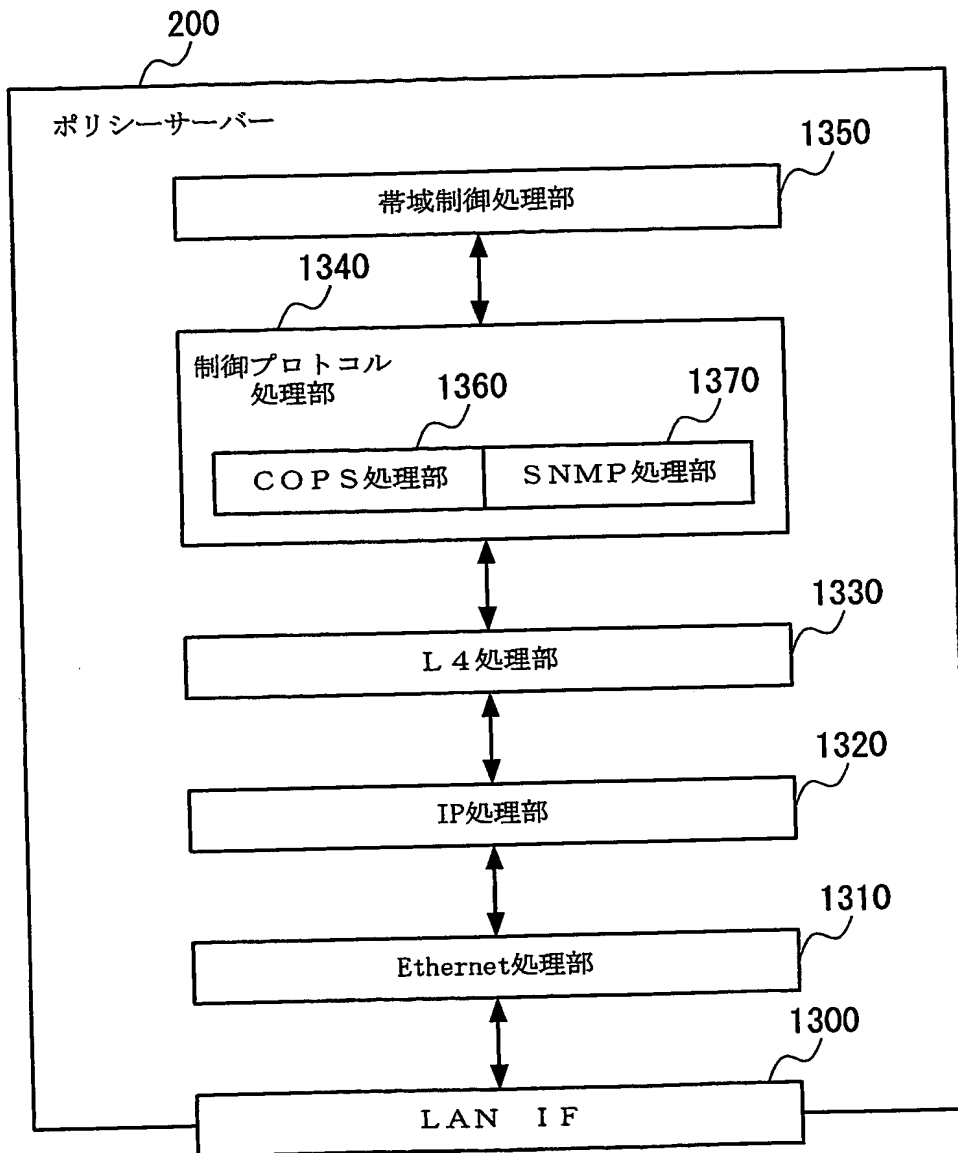
【図 4】



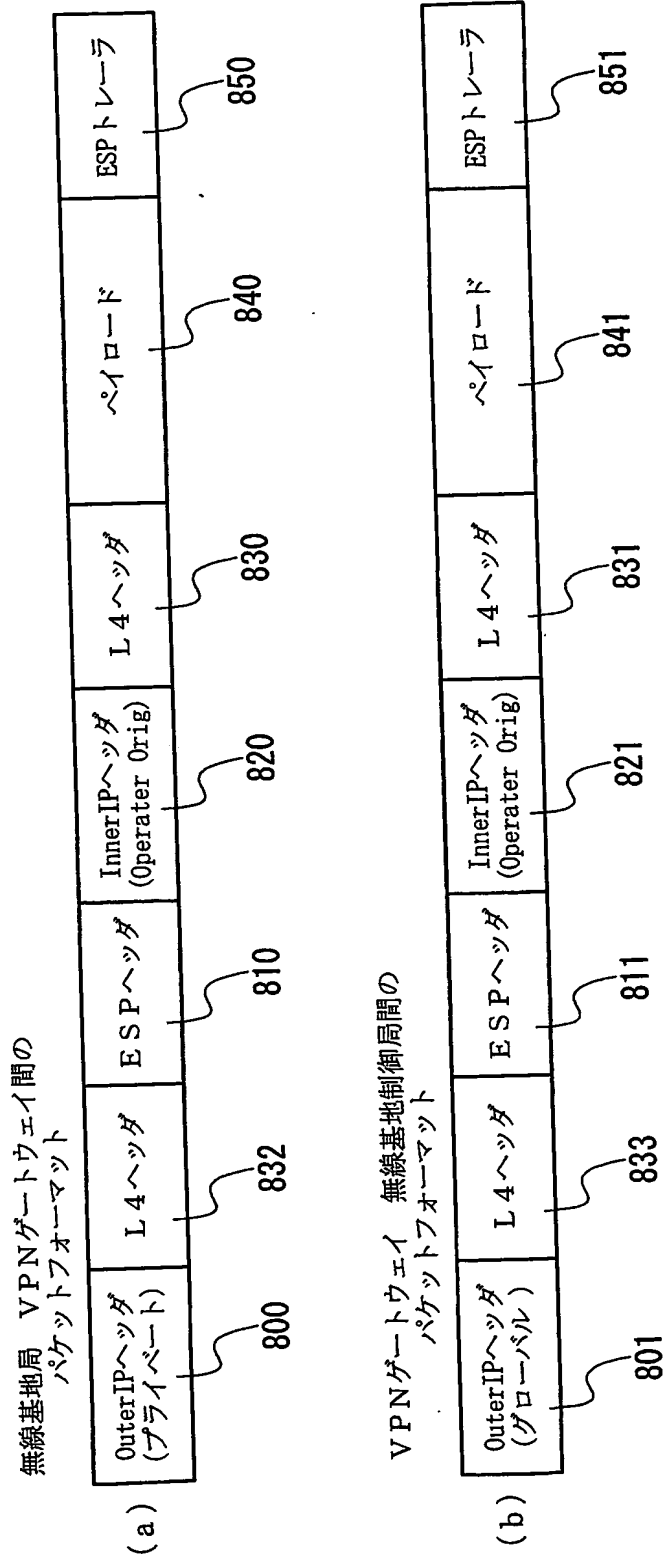
【図 5】



【図 6】



【図7】

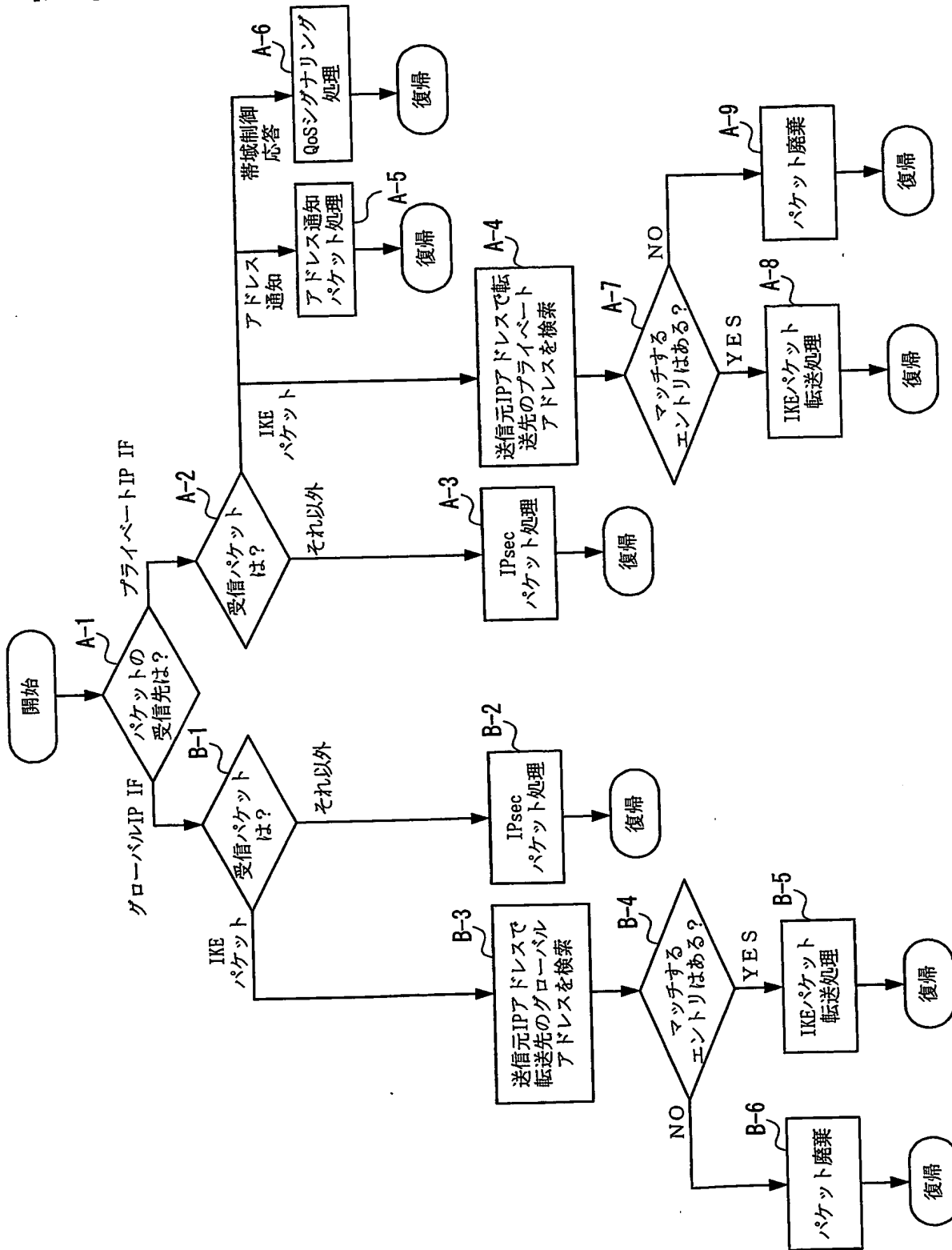


【図 8】

900 転送テーブル

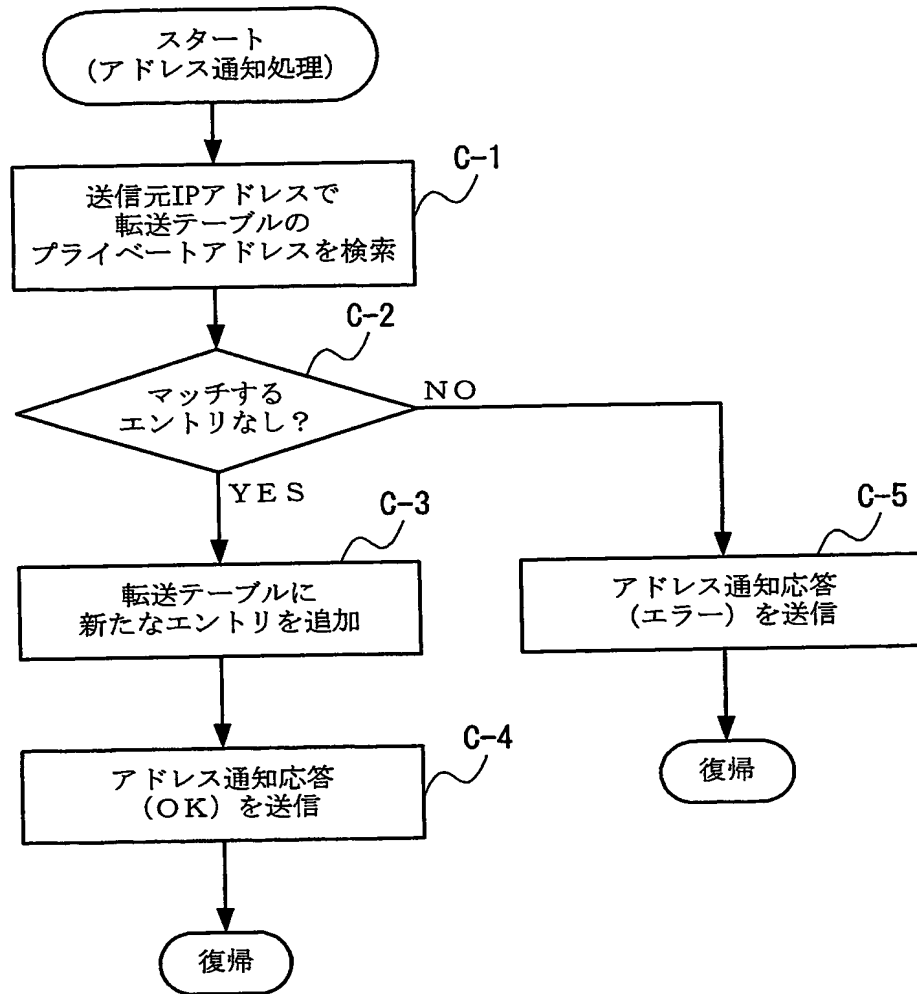
無線基地制御局		無線基地局	
グローバル アドレス	オペレータ独自 アドレス	プライベート アドレス	オペレータ独自 アドレス
aaa. bbb. ccc. ddd	mmm. nnn. ooo. ppp	eee. fff. ggg. hhh	mmm. nnn. ooo. qqg
		eee. fff. ggg. kkk	mmm. nnn. ooo. rrr
		eee. fff. zzz. yyy	mmm. nnn. ooo. sss
		eee. fff. zzz. xxx	mmm. nnn. ooo. ttt

【図9】

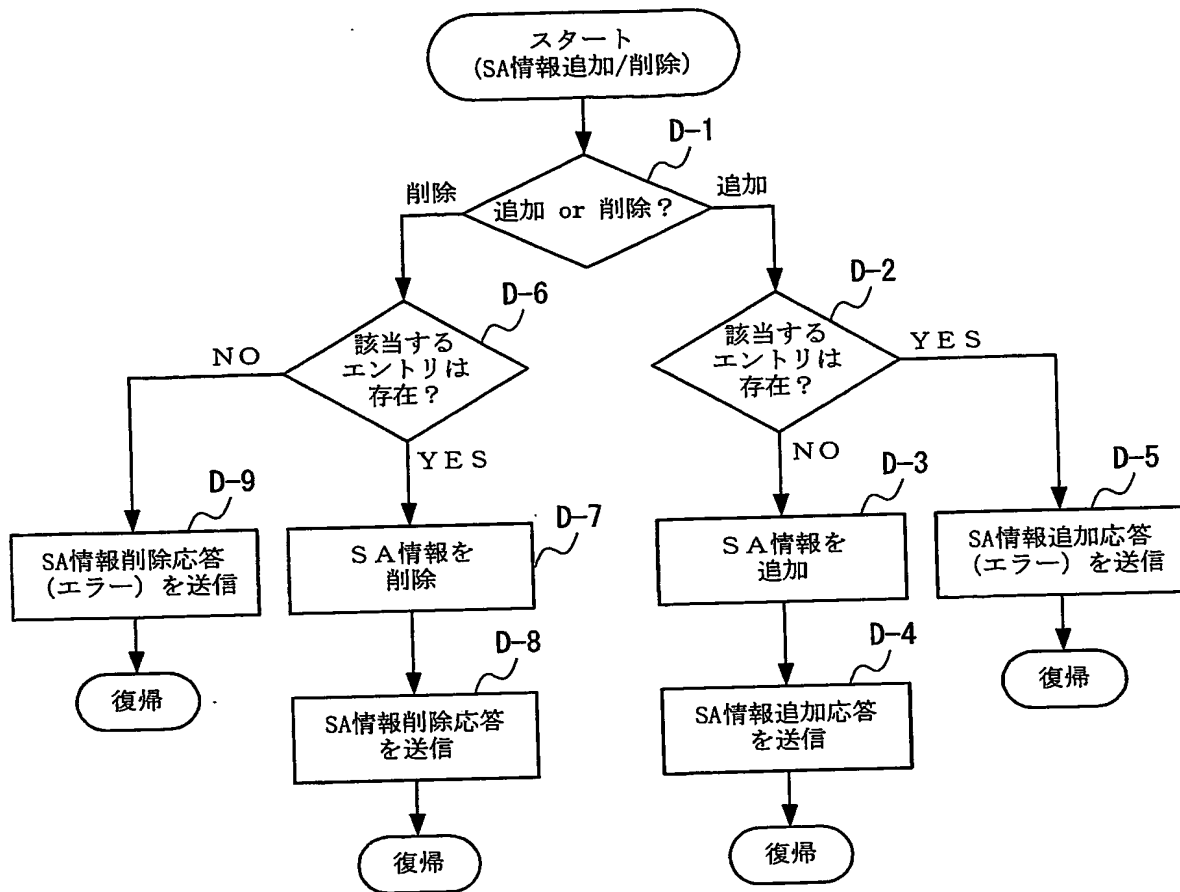




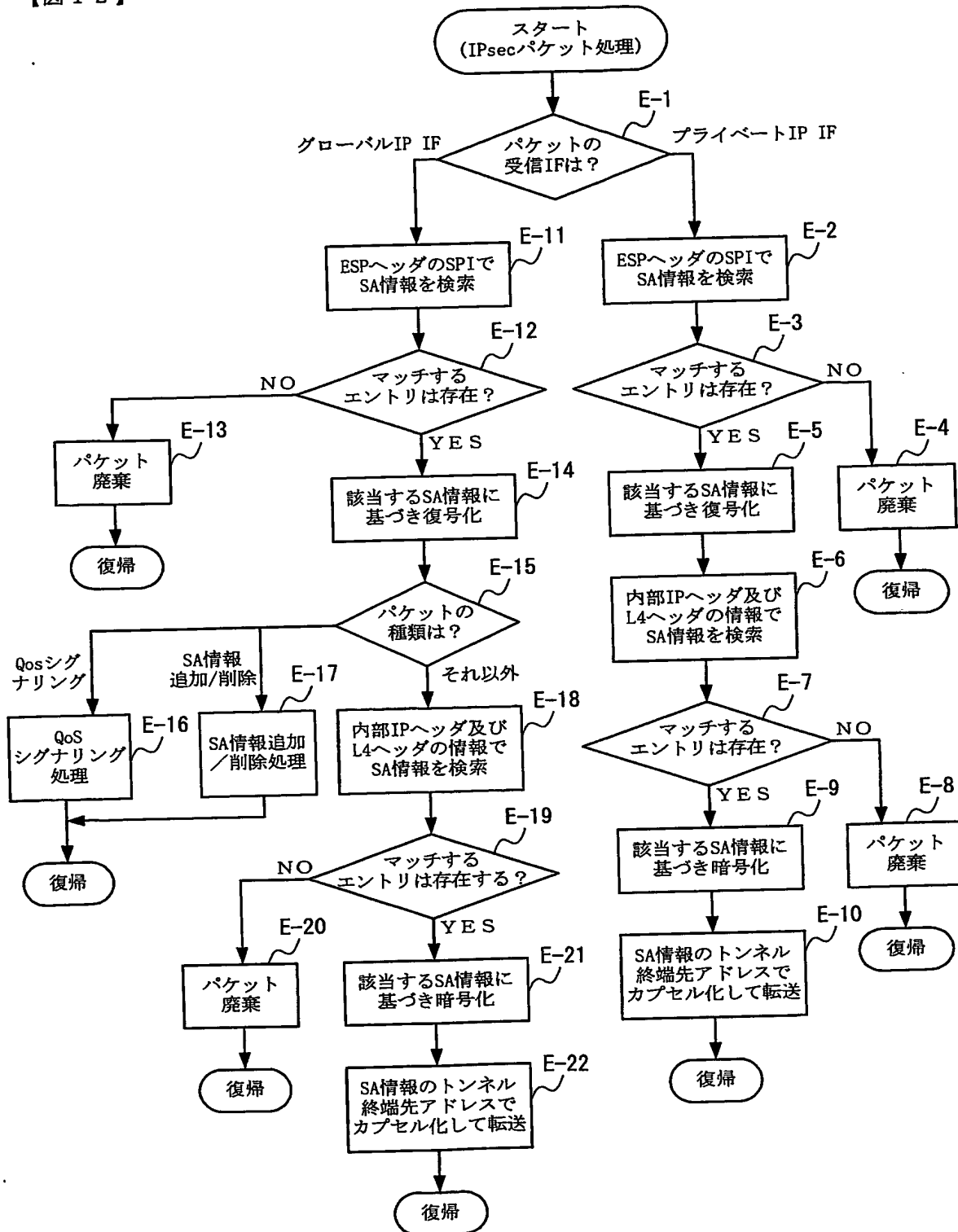
【図10】



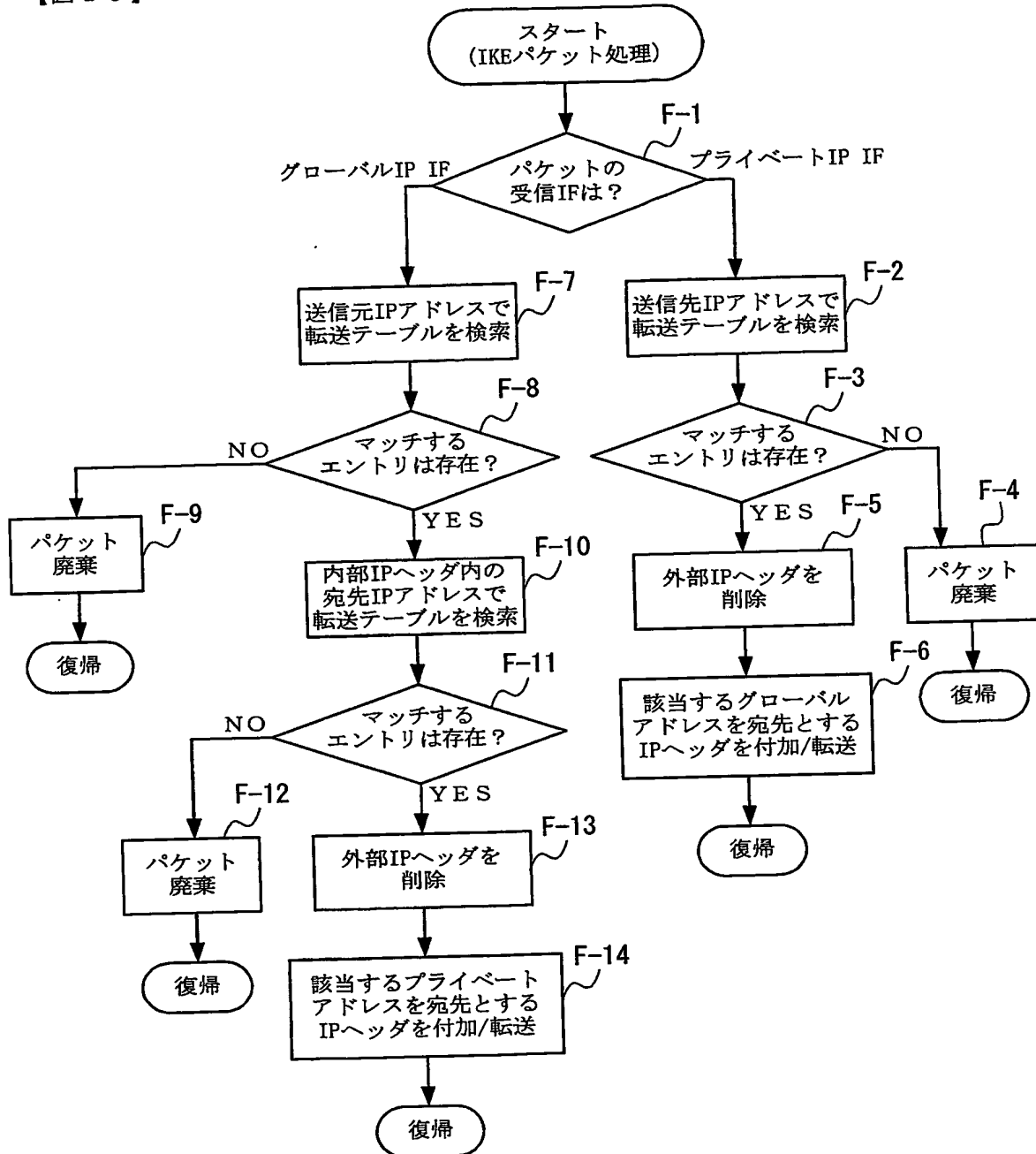
【図 11】



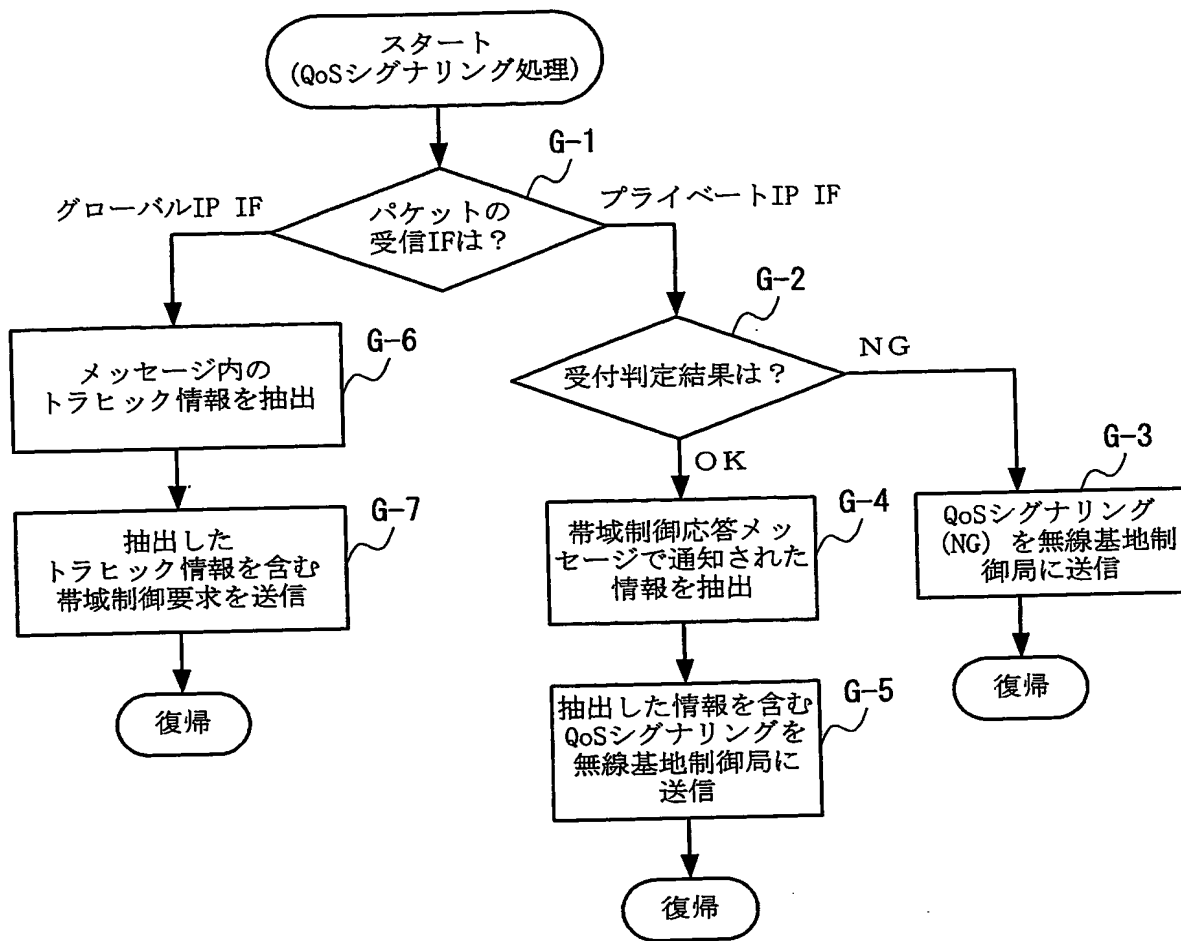
【図 12】



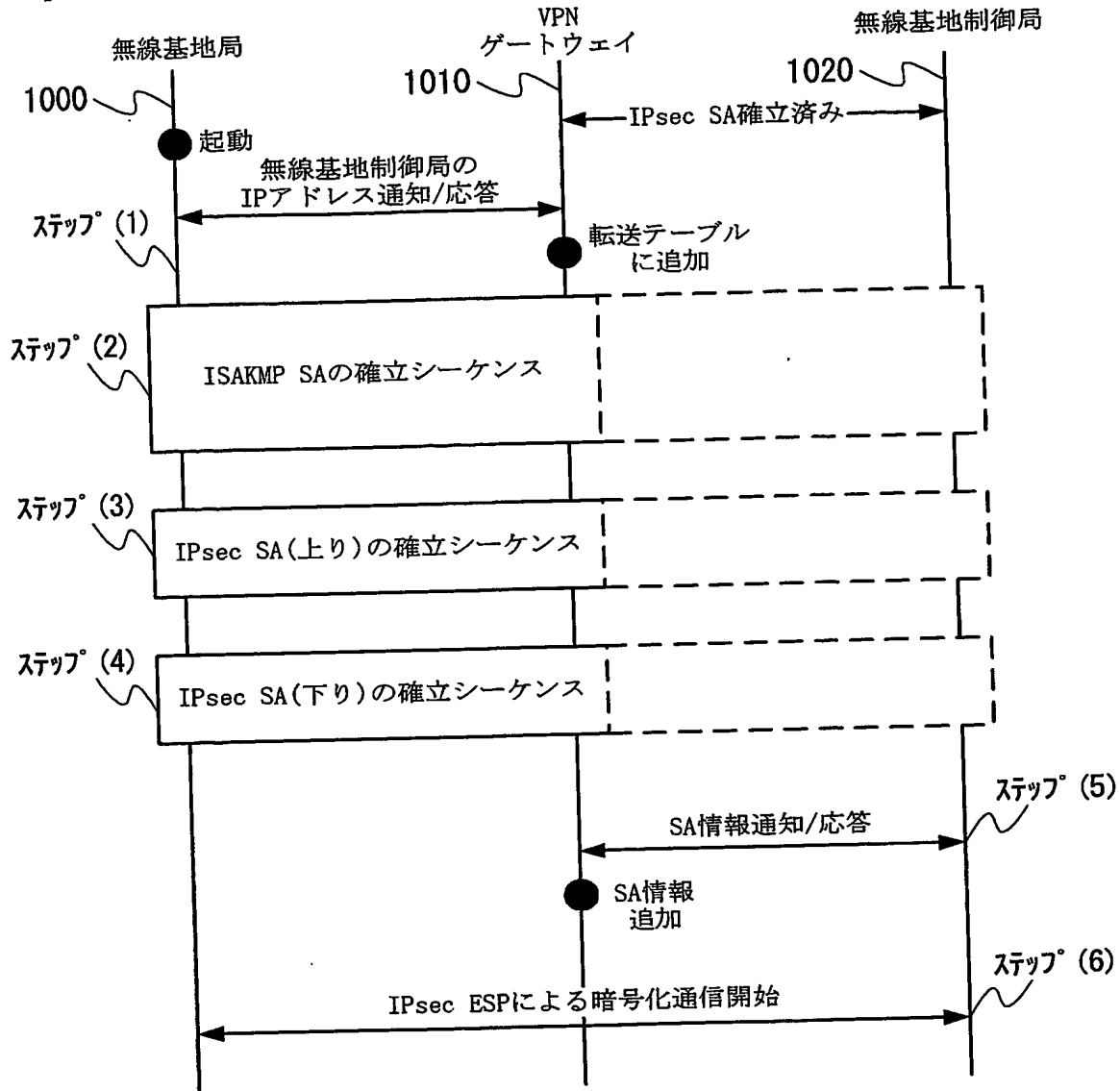
【図 13】



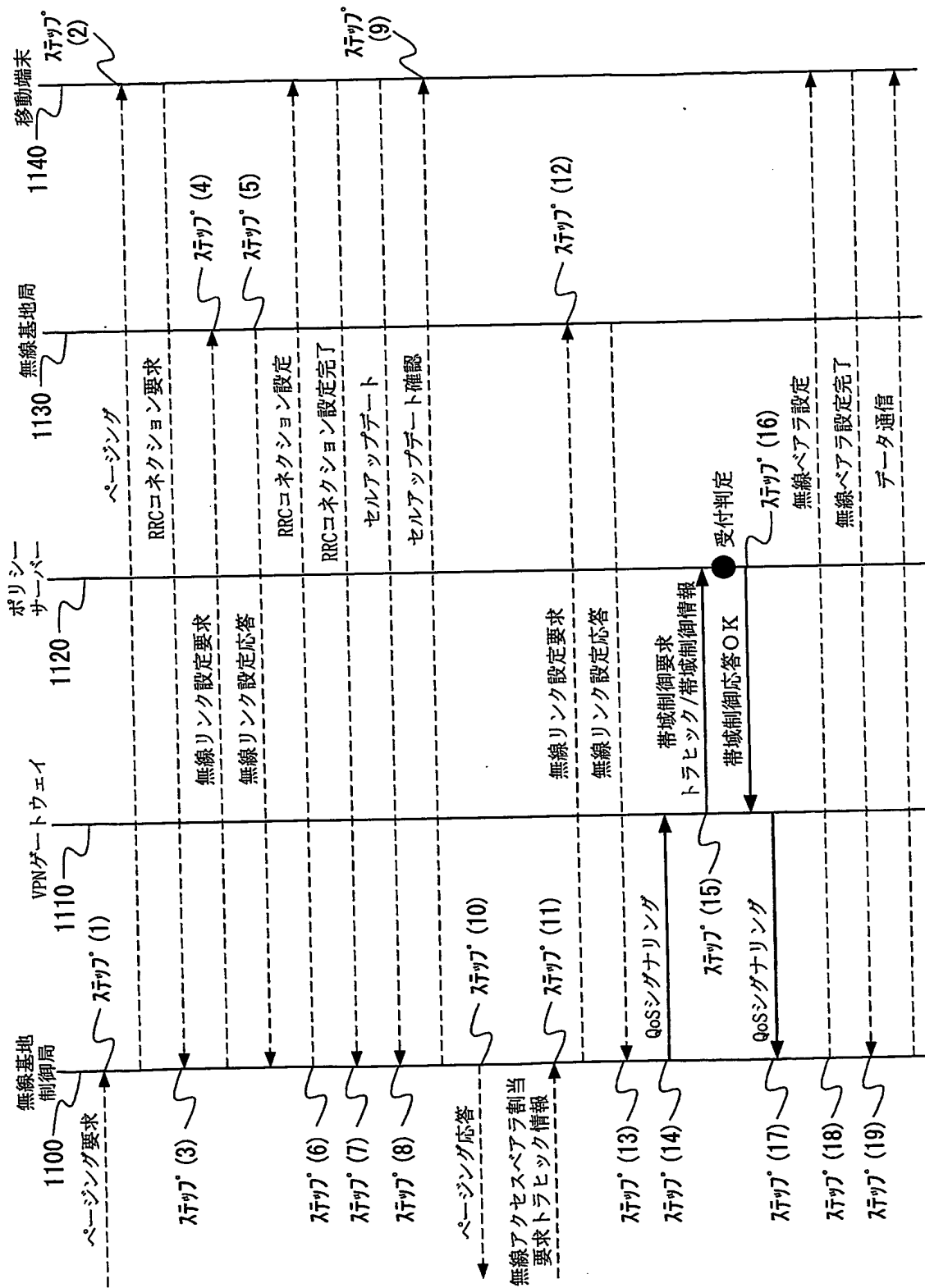
【図14】



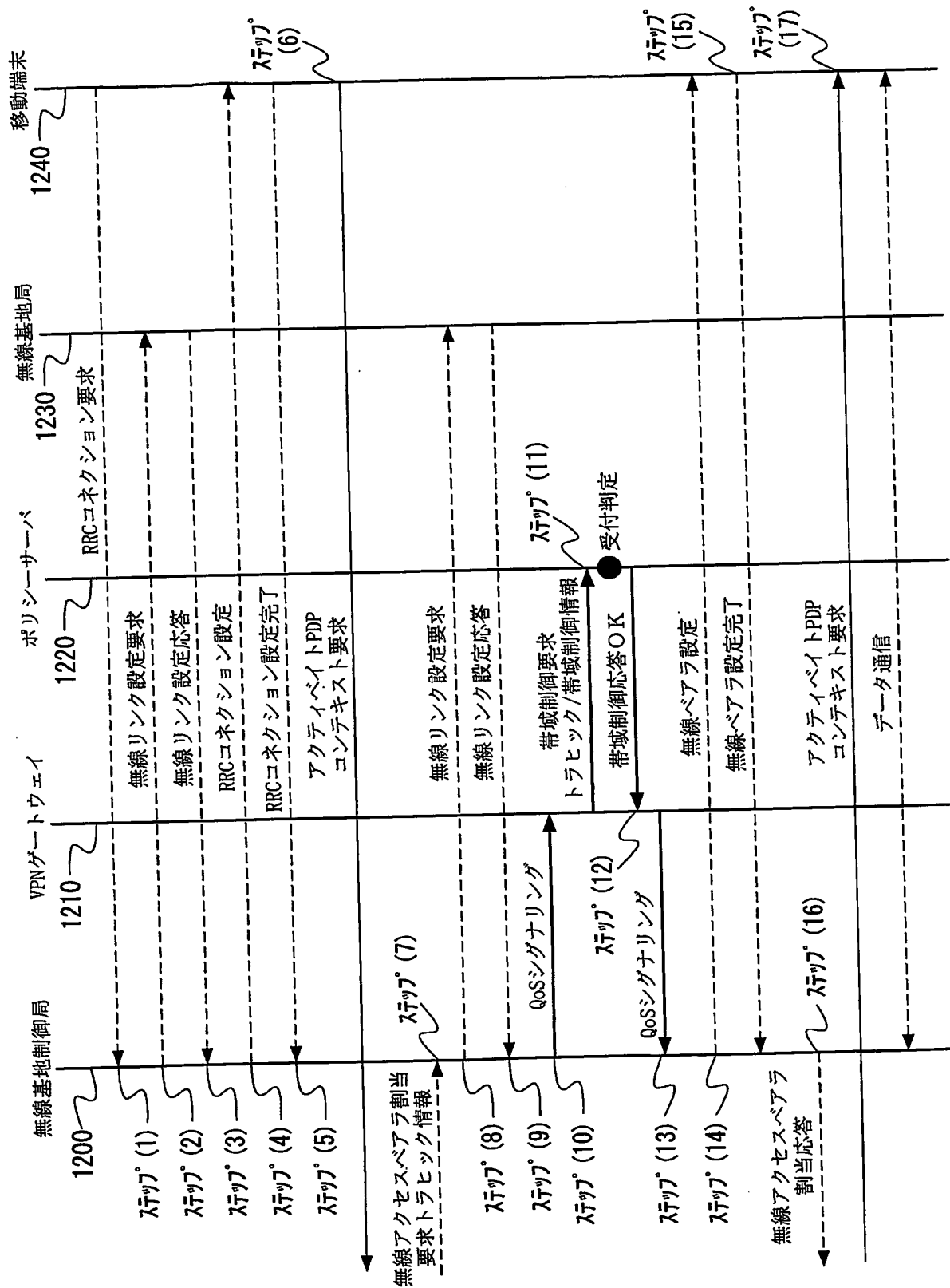
【図 15】



【図16】

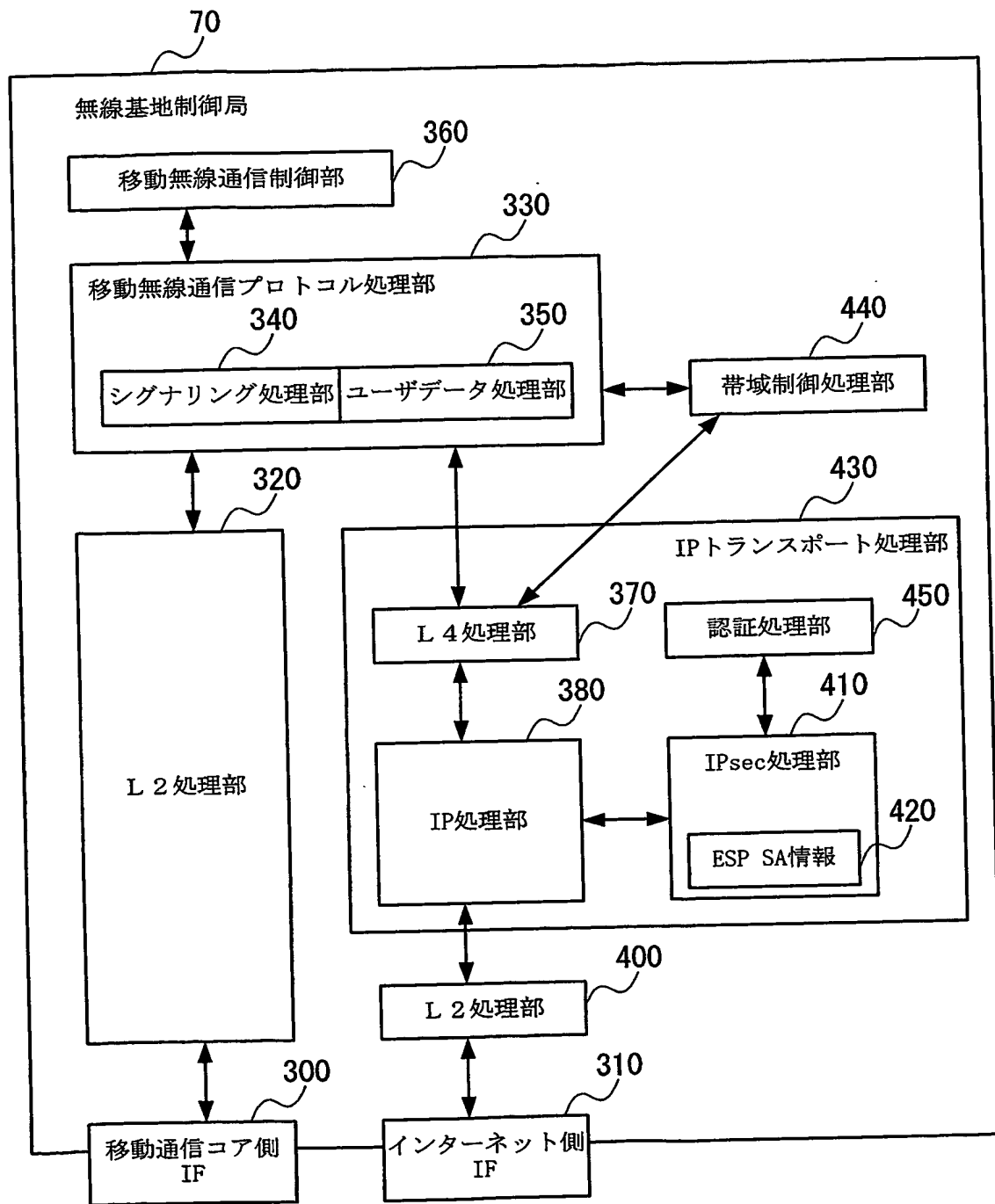


【図17】

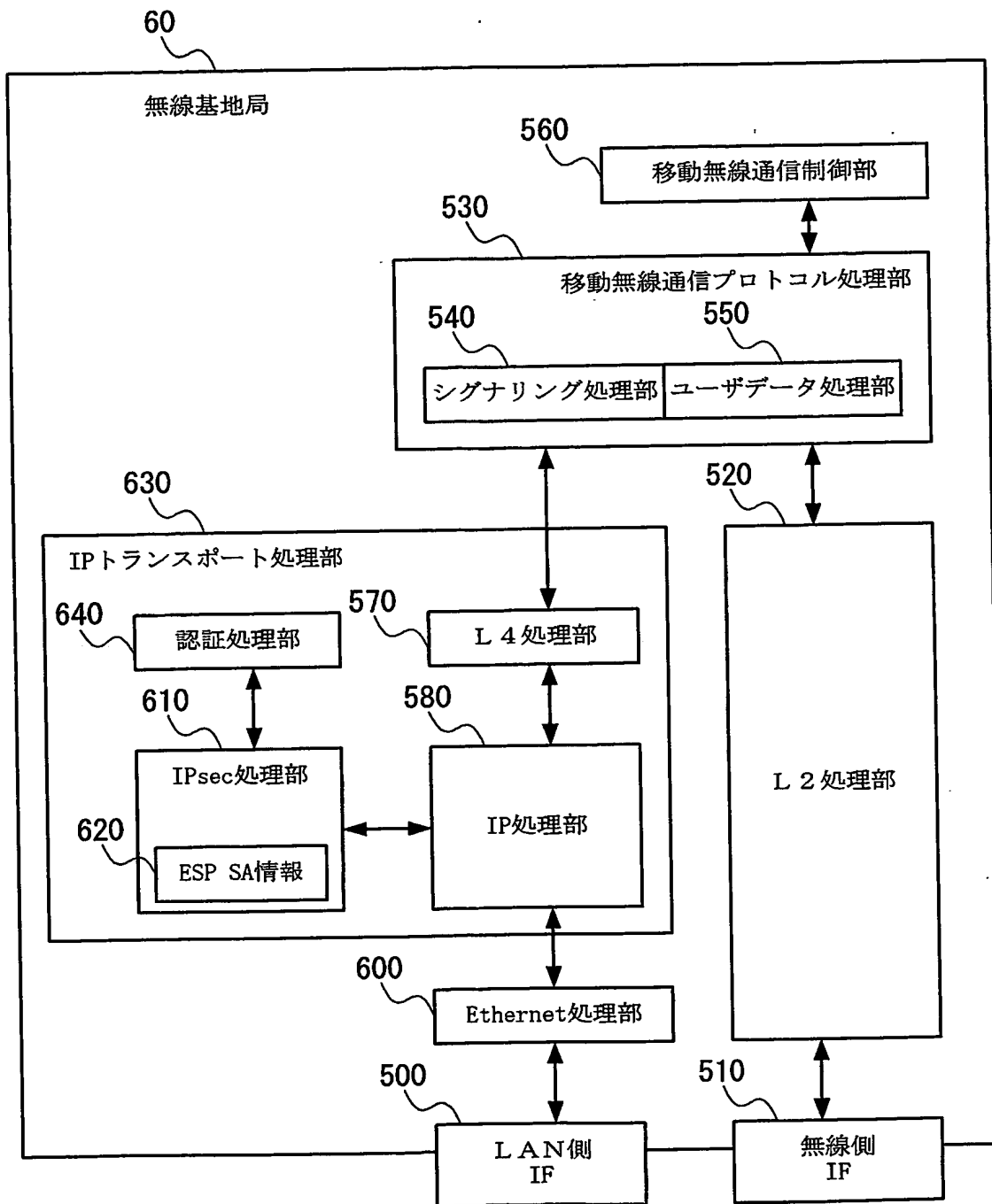




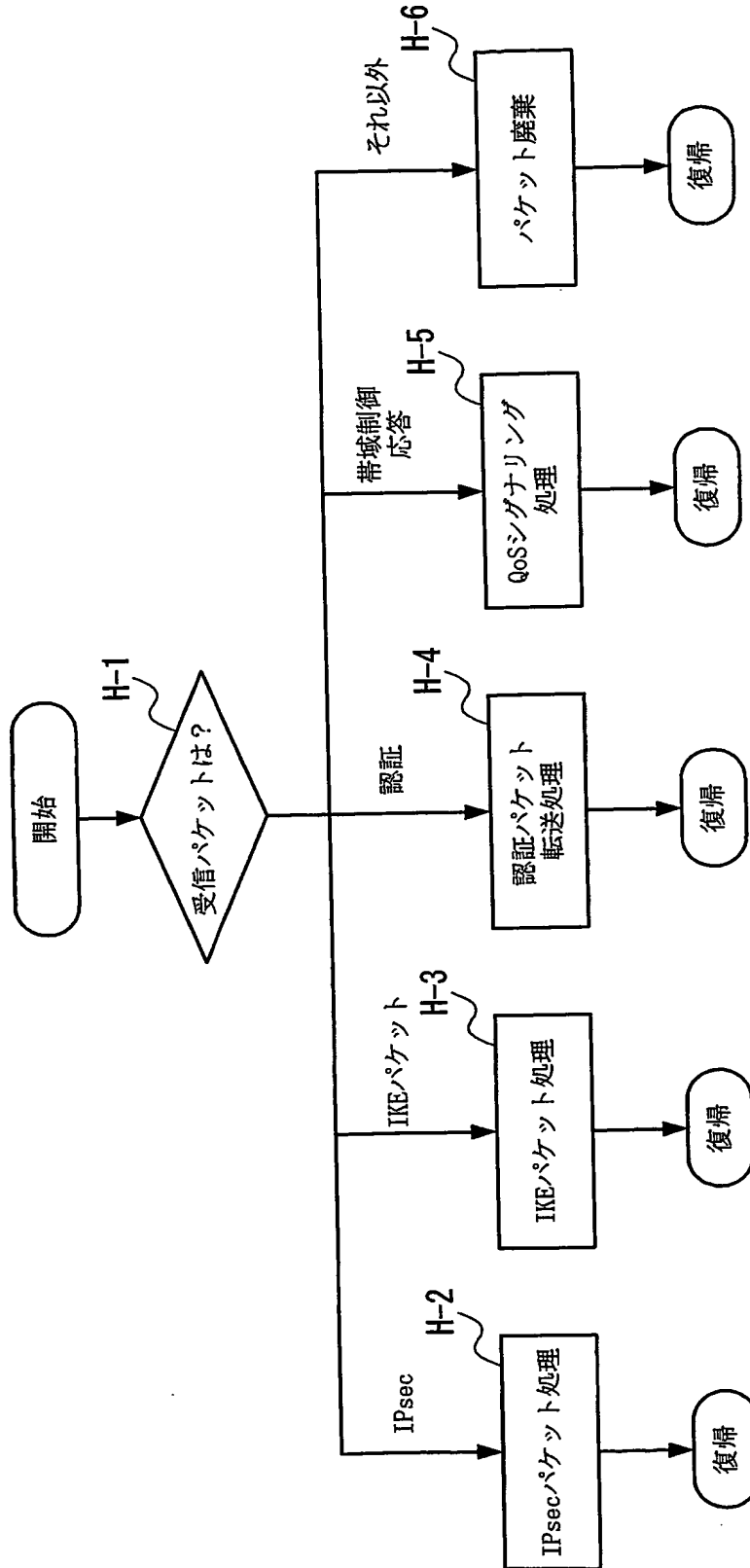
【図18】



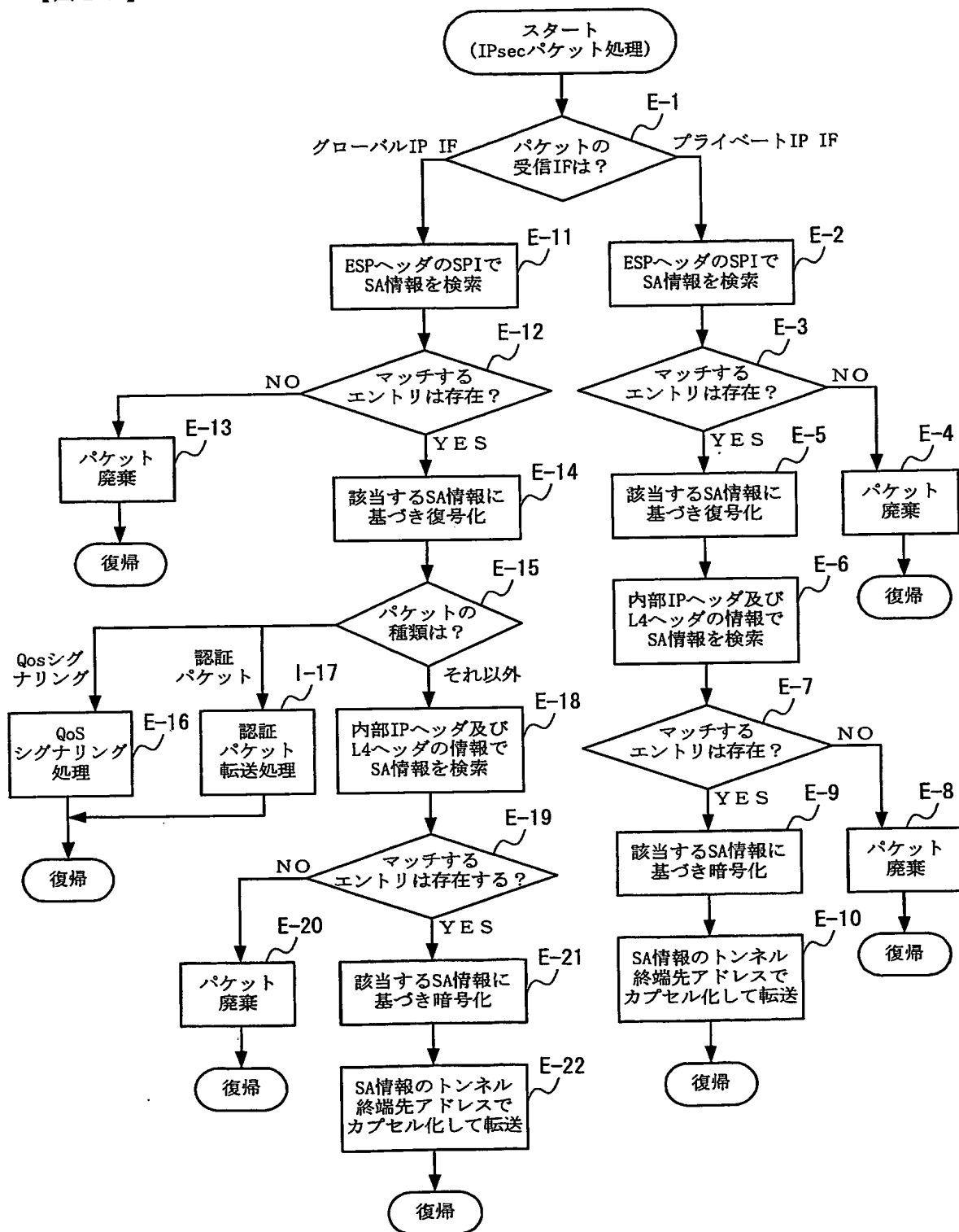
【図19】



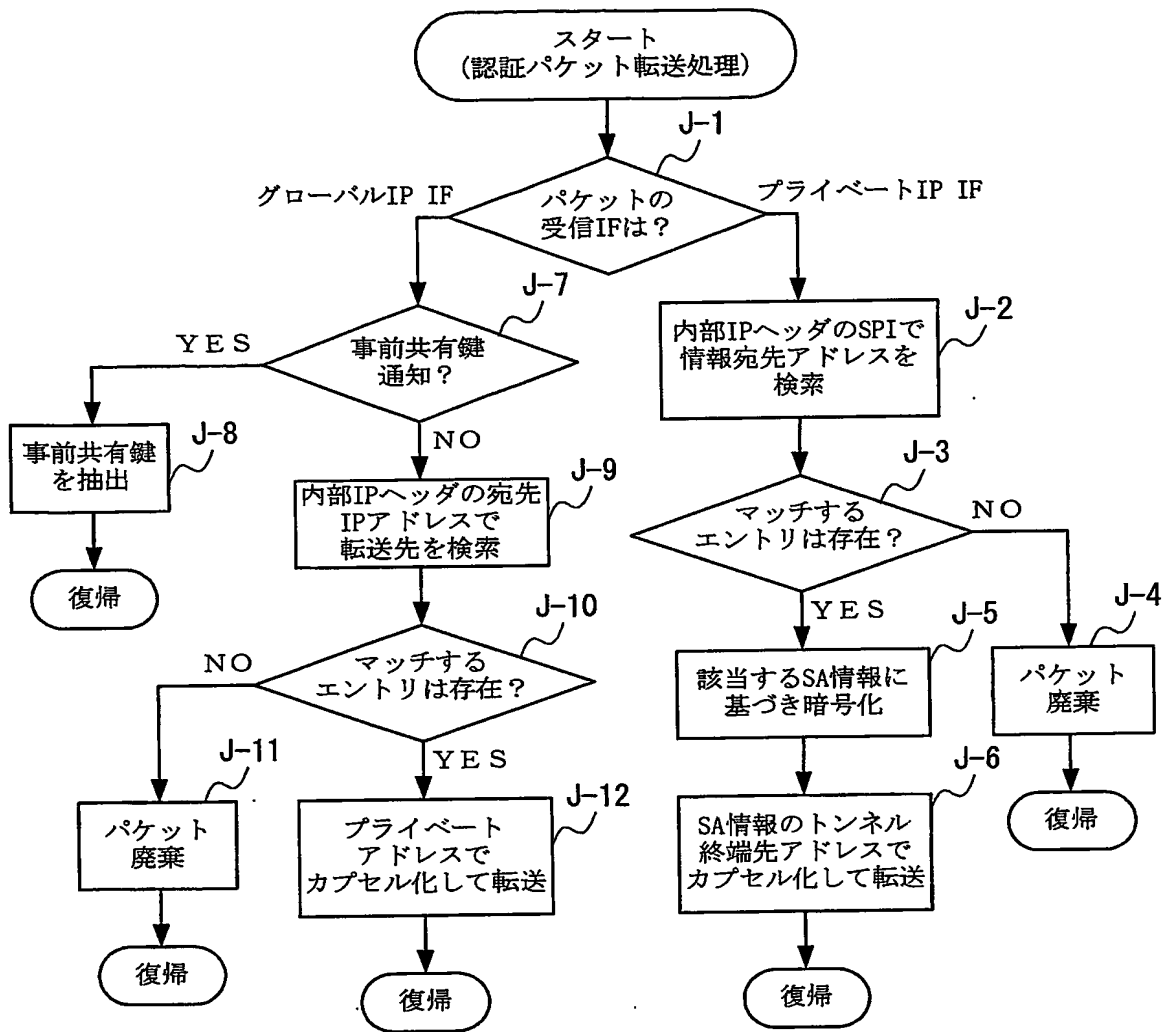
【図 20】



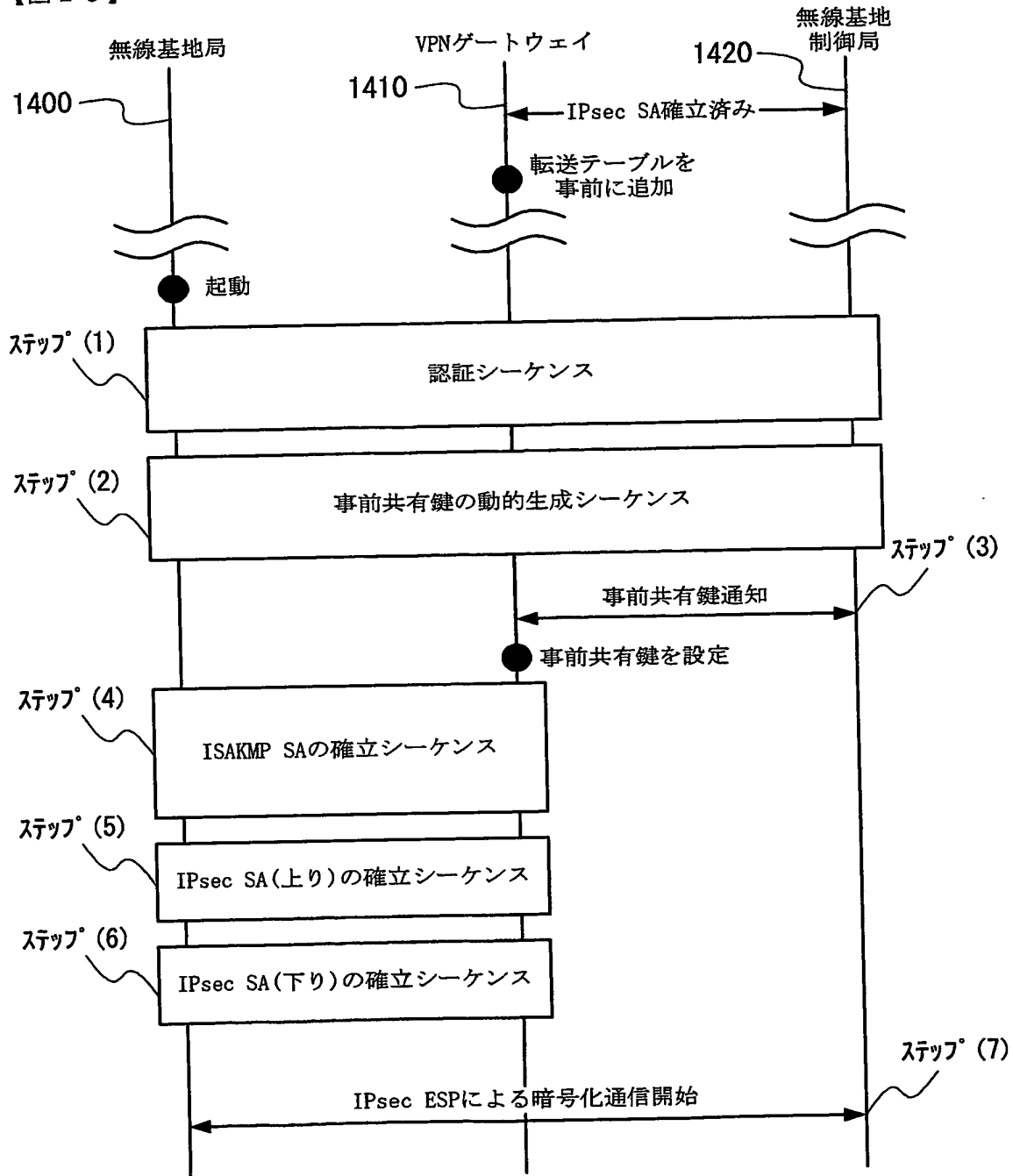
【図 21】



【図 22】



【図 23】



## 【書類名】要約書

## 【要約】

【課題】 私設網を用いて移動通信サービスを提供するに当たり、移動通信トラヒックの増大に起因して私設網内回線が輻輳するのを防ぎ、他のトラヒックにも支障をきたさない移動通信システムを提供する。

【解決手段】 移動端末 80 の発呼あるいは着呼時に、移動通信制御シグナリングを受信した中継ノードである VPN ゲートウェイ 100 が私設網である LAN 20 内の帯域制御機構と連携して受け付け判定を行い、受付が許可された場合のみ、移動端末 80 に通信回線を提供し、あるいは、無線基地局 60 と無線基地制御局 70 間で鍵交換メカニズムにより動的に事前共有鍵を生成し、無線基地制御局 70 が VPN ゲートウェイ 100 に事前共有鍵を通知する。

【選択図】 図 2

認定・付加情報

特許出願の番号	特願 2003-390216
受付番号	50301914384
書類名	特許願
担当官	第七担当上席 0096
作成日	平成15年11月21日

<認定情報・付加情報>

【提出日】

平成15年11月20日



特願 2 0 0 3 - 3 9 0 2 1 6

出 願 人 履 歴 情 報

識別番号

[ 0 0 0 0 0 4 2 3 7 ]

1. 変更年月日

1 9 9 0 年 8 月 2 9 日

[変更理由]

新規登録

住 所

東京都港区芝五丁目 7 番 1 号

氏 名

日本電気株式会社

**This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record.**

## **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

☒ **BLACK BORDERS**

☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**

☐ **FADED TEXT OR DRAWING**

☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**

☐ **SKEWED/SLANTED IMAGES**

☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**

☐ **GRAY SCALE DOCUMENTS**

☒ **LINES OR MARKS ON ORIGINAL DOCUMENT**

☒ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**

☐ **OTHER:** \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**